****

Healthcare and Public Health Vehicle-Borne Improvised Explosive Device Tabletop Exercise

Situation Manual

[Insert Date]

\*[Insert Caveat]\*

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.

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) Vehicle-Borne Improvised Explosive Device (VBIED) Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX, planned for [insert exercise duration], and will focus on [insert scope].  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 core 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** | VBIED |
| **Scenario** | An interactive, discussion-based exercise focused on a domestic VBIED 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 and 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 objective] | * [Insert capability aligned to each objective] |

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 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 [insert 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 [insert mission area] efforts. Problem-solving efforts should be the focus.
* The assumption is that 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

## [Insert Location]

### [Insert Month, Day, Year]: [Time]

Based on increased online chatter calling for targeted attacks on critical facilities, [insert local fusion center] identified a credible threat in [insert your region]. The threat appears to be an explosive event, though there is no threat of chemical, biological, or nuclear agents. There is a broad category of potential targets that include health care, law enforcement, fire, and EMS organizations.

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 indicates that domestic terrorists are sourcing precursor materials to construct IEDs and attempting to stockpile firearms. The alert is to remain in place for three months, ending on [insert date + three months].

### [Insert Month, Day, Year + 2 Weeks]: [Time]

The [insert your jurisdiction] Police Department receives a call from a concerned citizen reporting suspicious activity near [insert your facility name] earlier in the day. The citizen explains to police that while waiting for a friend, she observed an inconspicuously dressed man carrying a backpack and surveying the property. The individual also stopped several times in this time span to photograph the facility from multiple angles, focusing on the delivery loading dock. This individual’s activity lasted approximately 15 minutes. The citizen reports that shortly after she called the police, the man walked away, checking his watch every few seconds. He departs in a car just after an officer arrives to investigate the suspicious activity call.

The police department notifies [insert your facility name]’s building management and security of the incident, then inquires about any similar incidents and other suspicious activity that has taken place recently that might be related.

## 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 the departments within your organization?
   1. What do department heads do with this information?
   2. How does your organization protect suspicious activity information within your organization?
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 with similar types of venues?
   1. Would your organization alert other venues and facilities in the area to this situation?
8. How does your organization’s leadership share, receive, or coordinate information from independent sources?
   1. What process do media outlets use to relay received threat information to appropriate stakeholders?
   2. Who from your organization is responsible for communicating and coordinating with media outlets?
9. How does you organization communicate internally about credible threats?
   1. What protocols govern this communication process?
   2. How does your organization communicate this information to employees?
10. Do stakeholders in your organization receive instructions from leadership regarding what actions to take concerning imminent threats?
11. How would your organization alert individuals and organizations that use the facility, such as vendors, to this situation?
12. Does your organization conduct any specific training based on general or credible threats?
13. 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]

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

Your organization’s vehicle service provider reports a stolen vehicle to the police department. The police opened a case to search for the missing vehicle, though neither the company nor law enforcement have a potential lead to follow.

### [Insert Month, Day, Year + 21 Days]: [Time]

[Insert your facility name] is buy as usual. Your organization expect several equipment deliveries today and a few shipments have already arrived. A familiar truck is pulling into the loading dock when suddenly the vehicle accelerates and veers sharply to the right, over the curb, through employees, and directly into the loading dock, where it explodes. The crash throws back bystanders, and flying debris from the blast strikes them. The explosion causes a partial collapse of [insert number] floors of the building and ignites several small fires.

Many employees who were in [insert your facility name] at the time of the attack were able to escape through emergency fire exits, but they report that there are more seriously injured people still inside the building. Several victims seek out first responders and indicate that they could hear people calling out from the direction of the shattered lobby, though they could not see anyone through the smoke, dust, and rubble.

Law enforcement works quickly to secure the scene and clear the perimeter of the growing crowd. Within minutes, news outlets nationally broadcast footage from the explosion. Users on social media also share images and videos of the incident. Rumors spread of repeat attacks across the country, creating fear and panic. News media agencies and the public are clamoring for information. Calls from individuals searching for family and friends begin flooding office lines.

## Discussion Questions

1. Does your organization have an existing Emergency Operations Plan (EOP) that is adaptable to evolving threats?
   1. If so, how recently has your organization reviewed and updated the plan?
   2. Have you made local first responders aware of your EOP?
   3. Have local first responders ever visited your facility?
2. How does your organization alert employees to an incident?
   1. How does your organization alert local and state law enforcement to the incident?
   2. What emergency communications plan currently exists?
3. How do local, state, and federal agencies coordinate response operations?
   1. Who is responsible for this coordination?
4. What type of command structure would your organization establish?
   1. Who would be in charge of the command structure?
   2. What is the role of your organization and other private sector stakeholders in this command structure?
   3. Does your organization train employees on incident command procedures?
5. If such an incident occurred, what would be the role and responsibility of your organization’s security?
   1. What assets would security have on hand (guards, cameras, etc.)?
   2. Do specific procedures exist, or do more general emergency response plans address the actions of security guards?
   3. What are security’s priorities?
   4. With whom is your organization’s security communicating?
      1. Who is responsible for contacting local responders?
      2. Who is your organization notifying in your facility of the incident, and who is responsible for this?
      3. What systems does your organization use to communicate with first responders (in-person, radio, 911 / dispatch, etc.)?
      4. 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)?
   1. If so, who would staff the EOC in this incident?
7. What information would your organization pass on to the public?
   1. How quickly does your organization notify the public of the incident?
   2. Are there “canned / pre-scripted” messages for the public that your organization can easily edit to a specific incident?
   3. Who is responsible for this messaging?
   4. How do different agencies and organizations coordinate this messaging?
8. Does your organization have pre-identified Public Information Officers (PIOs)?
   1. Does your organization train PIOs for such incidents?
   2. Have your PIOs ever had the opportunity to work with local first responders and the jurisdiction’s PIOs?
   3. How does your organization integrate outside PIOs into the command structure?
   4. In addition to your organization’s public messaging efforts, would other organizations be providing public information?
      1. Realistically, when would your organization address public information?
      2. What would be your organization’s public information priorities following an incident?
      3. 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?
   1. If so, who is responsible for the accountability check? Who collects the information?
   2. What does your organization do if an employee does not respond?
   3. Do your organization’s plans and procedures outline this process? If so, are your employees aware of the existing plans and procedures?
10. What crowd control procedures exist for an incident of this type?
    1. Who is responsible for crowd control?
    2. Does your organization predetermine ingress / egress routes in case of an emergency like this?
    3. What directions, if any, would your organization give to the crowd?
    4. 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?
    1. Who makes the decision to evacuate of shelter-in-place?
    2. How does this person communicate the decision?
    3. Does your organization predesignate a rally point?
    4. Does your organization train employees in either of these responses?
12. How would your organization determine if this incident were a targeted, localized incident at [insert your facility name]?

This page is intentionally left blank.

# Module Three: Recovery

## Scenario

## [Insert Location]

### [Insert Incident Date + 1 Day]: [Time]

Law enforcement reported the scene secure and confirmed the suspect amongst the fatalities. There are estimates of at least [insert number] fatalities, [insert number] critical injuries, and multiple minor injuries.

The medical facility and 911 call centers continue to receive numerous requests for information about the incident from families and friends worried about loved ones. The incident affected multiple floors of the facility, making many areas inaccessible because of structural damage, scattered broken glass and metal, and exposed electrical wiring. Some employees and patrons are showing signs of trauma from witnessing coworkers and patients become injured from the blast.

## Discussion Questions

1. How does your organization determine the status of your facilities before, during, and after an incident?
   1. If your organization implements a lockdown, at what point would you lift it?
2. How does damage or disruptions to your operations impact surrounding organizations?
3. How does your organization manage resources during an event?
   1. How would a shortage of resources impact your facilities?
   2. How would your organization involve Crisis Standards of Care (CSC) and how would that impact recovery operations in this incident, if at all?
4. Do your organization’s plans, policies, or procedures specifically address resource management?
   1. What type of mutual aid agreements or memorandums of understanding (MOUs) do you have with surrounding hospitals to assist with patient care or resource shortages?
5. How does your organization reunite separated families?
   1. How quickly does your organization begin reunification procedures?
   2. Does your organization specify a location for walk-ins looking for loved ones?
   3. Do your organization’s plans, policies, and procedures outline this process?
   4. Would your organization consult the Red Cross to help facilitate family reunification?
6. How does your facility handle incoming calls from people searching for loved ones?
7. What are the priorities at your facility or organization post-incident?
   1. Do your organization’s plans, policies, or procedures specify these priorities?
   2. How does your organization communicate these priorities internally?
   3. Does your organization coordinate priorities with county emergency management?
   4. Does your organization coordinate priorities with state or federal agencies?
8. Whom would your organization inform when normal operations are disrupted?
   1. Who would need the information first?
   2. What information does your organization need to provide?
   3. How would your organization communicate this information?
   4. At what point would your organization distribute this information?
   5. Do your organization’s plans, policies, or procedures specify this information?
9. How does your organization recover from infrastructure impacts to maintain continuity of business operations?
   1. What continuity procedures does your organization have if employees are unable to work?
10. What information is your organization communicating to the public?
    1. Who in your organization is responsible for making this communication?
    2. Are there social media resources available during and immediately after an incident?
    3. What measures does your organization take to disrupt the distribution of misinformation?
11. What type of trauma counseling or mental health services does your facility offer following an incident, if any?
    1. Does your organization provide these services for both employees and patients?
12. How much time would your organization estimate is necessary to resume business?
    1. How long might an investigation take? How does it impact business continuity operations?
    2. How will your hospital receive situational updates from law enforcement?
    3. At what point would your organization consider your facility back to steady-state operations?

# Appendix A: Exercise Participants

| **Participating Private Sector Organizations** |
| --- |
| [Insert private sector participants] |
|  |
|  |

| **Participating Local Organizations** |
| --- |
| [Insert local participants] |
|  |
|  |

| **Participating State Organizations** |
| --- |
| [Insert state participants] |
|  |
|  |

| **Participating Federal Organizations** |
| --- |
| [Insert federal participants] |
|  |
|  |

| **Other Participating Organizations** |
| --- |
| [Insert other participants] |
|  |
|  |

This page was 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 |
| **CSC** | Crisis Standards of Care |
| **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 |
| **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 |
| **VBIED** | Vehicle-Borne Improvised Explosive Device |

Cybersecurity and Infrastructure Security Agency logo. Logo is circular and shows an eagle silhouette with the words "Cybersecurity and Infrastructure Security Agency" written around the circumference.  
