[Insert Cover Picture]

Outdoor Events Active Assailant IED 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 Intelligence and Information Sharing |
| 9:45 a.m. | 9:55 a.m. | Break |
| 9:55 a.m. | 10:55 a.m. | Module Two: Incident and Response |
| 10:55 a.m. | 11:05 a.m. | Break |
| 11:05 a.m. | 12:05 p.m. | Module Three: Short-Term 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** | Outdoor Events Active Assailant IED 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 * Intelligence and Information Sharing * Mass Care Services * Operational Coordination * On-Scene Security and Protection * Planning * Public Information and Warning * [Insert other core capabilities as necessary] |
| **Objectives** | 1. Examine pre-incident and incident intelligence and information sharing procedures between public and private sector stakeholders. 2. Review emergency preparedness plans and response procedures to an attack on an outdoor event. 3. Discuss the coordination between private sector organizations and responding local, state, and federal agencies under the National Incident Management System (NIMS). 4. Assess procedures for coordinating and sharing information within organizations, between organizations, and with the public. 5. Review organizational interdependencies and recovery plans. 6. [Insert additional exercise objectives as necessary] |
| **Threat or Hazard** | Vehicle Ramming, Active Shooter, Improvised Explosive Device (IED) |
| **Scenario** | An interactive, discussion-based exercise focused on an attack on an outdoor event. The scenario consists of three modules: Pre-Incident Intelligence and Information Sharing, Incident and Response, and Short-Term 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 pre-incident and incident intelligence and information sharing procedures between public and private sector stakeholders. | * Intelligence and Information Sharing * Planning * Public Information and Warning |
| Review emergency preparedness plans and response procedures to an attack on an outdoor event. | * Mass Care Services * Operational Coordination * On-Scene Security and Protection * Planning * Public Information and Warning |
| Discuss the coordination between private sector organizations and responding local, state, and federal agencies under NIMS. | * Operational Coordination * Planning |
| Assess procedures for coordinating and sharing information within organizations, between organizations, and with the public. | * Operational Communications * Planning * Public Information and Warning |
| Review organizational interdependencies and recovery plans. | * Economic Recovery * Planning |
| [Insert additional objectives as necessary]. | * [Insert additional 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 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 Intelligence and Information Sharing
* Module Two: Incident and Response
* Module Three: Short-Term 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 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 Intelligence and Information Sharing

## Scenario

## [Insert Location]

### [Insert Month, Day, Year]



In the last few weeks, there has been an increased amount of online chatter from the domestic extremist group, Universal Adversary (UA), calling for attacks on large public gatherings across the United States. Based on the posts, the Secretary of Homeland Security, in coordination with other federal entities, issues an “Elevated” Threat Alert through the National Terrorism Advisory System (NTAS), warning of a credible domestic terrorist threat across states in several identified areas. There is no information at this time that would warrant the release of an “Imminent” Threat. The alert is to remain in place until further notice.

With your event quickly approaching, members of the [insert law enforcement / intelligence agency] begin noticing posts on social media platforms from a small subset of individuals empathizing with UA’s calls for aggression. While no one has specified what actions they might take, posts and comments online have included warnings that the town “will get what’s coming to them.”

Based on the comments and posts, investigators suspect a violent incident may take place during the event. [Insert law enforcement / intelligence agency] immediately disseminates a suspicious activity report (SAR) with screenshots of the posts to the venue and local law enforcement.

## Discussion Questions

1. How would your agency or organization expect to receive information about a credible threat?
   1. How would you expected to receive NTAS alerts?
   2. Are there any government clearance considerations or issues when receiving or sharing threat information?
2. What information does your organization or agency expect from the intelligence community and local, state, and federal partners regarding threats of this nature?
3. How will your organization receive this information?
4. How long does it take for your organization to process information for sharing?
5. What security recommendations are public sector partners making to private sector partners?
6. How does your agency or organization triage intelligence information you receive, such as from formal reporting, hearsay, and social media?
7. What social media monitoring does your agency or organization conduct?
   1. How would this NTAS alert affect social media monitoring?
   2. How is this type of alert, or any suspicious activity alert, communicated to the departments within your organization?
   3. What do department heads do with this information?
8. How would law enforcement or fusion centers disseminate this information?
9. How would this NTAS alert affect preparations for upcoming sporting events?
   1. What actions, if any, would your organization take in response to this alert?
   2. How would this alert information change your organization’s incident response readiness?
   3. What protective measures or actions, if any, are put into place following this alert?
10. What kind of messaging would be released to the public, organizational leaders, and venue users?
    1. What would trigger this information sharing?
    2. Who is responsible for releasing the information / messaging?
11. What training, if any, does your agency or organization conduct based on credible threats?
12. Does this training include emergency management or active shooter elements?
13. Does your organization conduct any cross-training with local law enforcement or other first response agencies?
14. Does this training include the Incident Command System (ICS)?
15. Is your organization aware of SAR?
    1. Is SAR training provided within your organization?
    2. How would your organization implement SAR protocol in the wake of last month’s NTAS alert?
16. What would law enforcement officials expect to do with SAR intelligence information?
    1. How would this information be disseminated, and to whom?
17. Once informed of a credible threat, what information is law enforcement sharing with other public and private sector organizations that could be at risk?
18. What steps does your organization take once you receive notice of a possible or credible threat?
19. How would threat information be communicated within your organization? Would it include key organizational leadership?
20. What are you communicating to your employees?
    1. How is information shared with your employees?
    2. Who in your organization is responsible for addressing employee concerns?
21. How is this information shared with the customers or stakeholders who use your facility?
22. What information sharing protocols exist between organizations? How would other sporting venues in the area be alerted to this situation?
23. How would additional threat information change your organization’s / agency’s security posture?
    1. What additional protective measures are put in place following this threat information?
    2. Would you conduct additional hazard- or threat-specific training?
24. What security recommendations, if any, are law enforcement agencies making to private sector stakeholders?
    1. What other information is law enforcement sharing with private sector stakeholders?
25. What plans exist describing the required protective measures that need to be taken prior to the event?
26. Are there any notifications that need to be made outside of your organization?
    1. Are there any notifications that need to be made to the media?
    2. Who is responsible for disseminating this information to the appropriate parties?

This page is intentionally left blank.

# Module Two: Incident and Response

## Scenario

## Location: [Insert City / County, State]

### [Month, Day, Year]

The [insert event name] is the largest fair in the state and is held annually in the county seat of [Insert County]. It is a three-day event that showcases local products and handiwork during the day, with music, dancing, and entertainment at night. The fair is spread over a multi-block radius within the historic downtown area and along a mile-long stretch of the road leading to the county fairgrounds.

At 2:31 p.m. on Saturday, the second day of the fair, the [Insert County] Police Department receives a credible bomb threat targeting the downtown building that houses the event headquarters and main art exhibit. As [insert law enforcement agency / personnel type] begin initial investigations and enact evacuation procedures, scrambling fair attendees spill out of the building and into the neighboring streets, mixing with people the commotion is attracting.

At 2:38 p.m., a man drives a large pickup truck down a side street, crashes into the downtown area, and plows into the gathering crowd. The truck collides with another vehicle and stops, leaving a swath of killed and injured people.

After the truck comes to a stop, there is a brief pause as the driver of the truck staggers out carrying a rifle and wearing a holstered pistol. He opens fire into the crowd and forces his way into an adjacent two-story building, where he continues to shoot people inside. He makes his way to the second floor, which has many windows with views up and down two streets and overlooks a park on one side. He moves from window to window, shooting at people in the streets and in the park until responding officers confront him, at which time he fatally wounds himself.

As the crowd runs in panic, some notice a large bag with wires sticking out of it in the passenger seat of the truck and begin yelling that there is a bomb.

## Discussion Questions

1. What plans, if any, are in place to prevent or deter an attack at your event?
   1. What plans exist to deter a vehicle intrusion?
   2. What plans exist to deter an active shooter (e.g, screening, security presence)?
   3. What plans exist to deter an IED?
2. How does event management staff and train on-site security for this event?
   1. Does this include cross-training with law enforcement?
3. Do the event organization’s standard operating procedures (SOPs) include incident response roles and responsibilities for event staff?
4. What assets are on-site to immediately respond to an incident?
   1. Are there volunteer organizations or other partner groups that would have resources who would participate in the immediate response?
5. What are your crowd control and evacuation procedures for an event of this type?
   1. Who is responsible for activating and executing the evacuation procedures?
   2. Are there secondary and tertiary rally points in case the primary point is part of the incident or evacuees overwhelm it?
   3. What plans or procedures exist to assist individuals with access and functional needs?
   4. What are the procedures for evacuating very important persons (VIPs) such as performers or visiting elected officials?
   5. Do your plans include accountability procedures for event staff?
6. How is incident information communicated?
   1. What notification methods (e.g., alerts, emails, telecommunications, text messages, special tools) are used to send alert information?
   2. What would the messaging say?
   3. What protocols exist for alerting event staff to an incident? Are contract employees and vendors included in this messaging?
   4. What protocols exist for alerting partner organizations to an incident?
   5. Who is responsible for sending out the alerts or warnings?
   6. Do you send out any notifications to the public using social media? If so, at what point in the incident would you expect to start sending the notifications?
7. What does immediate incident command look like for this incident?
   1. How do each of the relevant agencies integrate into the command structure?
   2. Are key agencies and event personnel familiar with the ICS?
   3. How would command be distributed among the different threats in this incident?
8. What plans exist to address a potential IED?
   1. Does law enforcement have any SOPs that would affect other entities (e.g., moving fire / emergency medical services (EMS) personnel out of an IED blast radius after discovering the explosive taking over nearby businesses for command posts or sniper positions, etc.)?
   2. How are on-site security (event / private) trained to respond to an IED?
9. How would your organization conduct the medical response?
   1. Which organizations and agencies would involve themselves in medical response operations?
   2. Has your organization established a mass casualty plan for this event?
   3. How and when would you communicate this incident to hospitals?
   4. Who is responsible for contacting the hospitals?
   5. At what point would first responders’ protocols allow medical personnel to enter the scene and begin triage and treatment of the injured?
   6. What impact would a potential IED have on EMS response?
10. What information or warnings would your organization release to the public?
    1. Would responders activate a Joint Information Center (JIC)?
    2. How do the different agencies and organizations coordinate messages before activating the JIC?

## Scenario Update

### Saturday Afternoon, [Month, Day, Year]: [Time + 2 Hours]

After investigation the bomb squad renders the IED safe. The attack left [insert number] people killed and [insert number] people wounded, with [insert number] of those in critical condition. [Insert County] fire, EMS, and hospitals are overwhelmed with patients.

Media personnel have surrounded the scene, with personnel capturing videos of the carnage and interviewing victims or those involved in the response. Social media is also rampant with photos and videos of the scene and posts sharing misinformation and speculation about the incident.

## Discussion Questions

1. Does your organization (public or private) have mutual aid agreements (MAAs) in place with other organizations?
   1. Are these agreements formal or informal?
   2. What are the financial considerations when requesting mutual aid?
2. What communications procedures would be occurring at this point of incident response?
   1. What communication methods (e.g., alerts, emails, telecommunications, text messages, and special tools) do event organizers and other private sector organizations use to share information?
   2. Do you use social media to communicate with the public? Who is responsible for those posts and for continued social media monitoring?
3. Who is responsible for notifying state or federal agencies to the incident, and at what point in the incident would this occur?
   1. What resources or actions would you expect from state or federal agencies?
   2. How would arriving state and federal resources integrate into the command structure and at which locations (unified command, area command, emergency operations center (EOC), multi-agency coordination (MAC) group, etc.)?
4. What role do city and county governments play in this scenario?
   1. Have local agencies established protocols with elected officials so that they know what to expect during incident response? And so local agencies know what elected officials’ priorities are?
   2. Is there a location (such as the EOC) where elected officials will know to go during an incident?
      1. If so, where is it?
   3. Have local agencies briefed elected officials on ICS?
5. Does your organization have a designated public information officer (PIO)? If so:
   1. Do protocols exist for addressing media inquiries?
   2. How does the PIO receive information about the incident?
   3. Does the PIO have pre-built templates for use in different kinds of emergencies?
   4. Is your PIO properly trained to address media inquiries both electronically and in person?
   5. Would your organization use social media during an incident?
6. At what point, if any, would a JIC be stood up?
   1. Who would be included in the JIC?
7. Do you know how to contact your CISA protective security advisor (PSA)?

This page is intentionally left blank.

# Module Three: Short-Term Recovery

## Scenario

### Saturday Evening, [Insert Date]

Early in the evening, the governor calls to express his condolences and provide details on what the state is doing to respond. Shortly thereafter, state and federal agency representatives begin to arrive on-scene. At the press conference, the mayor expresses his grief to reporters across the country and outlines what steps the city is taking to manage the incident. National reporting is focused on the attacker’s motivation; however, law enforcement is continuing to investigate and has not currently reached a conclusion regarding motivation.

## Discussion Questions

1. How would the command structure evolve over the course of the afternoon and evening?
   1. Which agencies would involve themselves in unified command?
   2. In addition to unified command, which agencies would have their own command centers set up in other locations?
   3. How would the EOC interface with unified command (phones, radios, liaisons, etc.) and how would participants define their roles?
   4. Would responders stand up a MAC group, and if so, when?
   5. How would arriving mutual aid agencies integrate into the command structure and at which locations (unified command at the scene, EOC, hospital, etc.)?
   6. What is the role of private sector stakeholders in this command structure?
      1. Have they received training on incident command procedures?
      2. Have public agencies crossed-trained with the private sector’s incident priorities?
2. Are there plans for establishing mass care facilities, family assistance, or reunification centers?
   1. Who is responsible for enacting these procedures?
   2. What outside organizations would need to be brought in to assist?
3. If [insert appropriate decision-making agency / organization] were to declare this incident a terrorist incident, what impact would that have?
   1. How would that impact federal and state involvement?
4. What steps does your organization need to take to ensure the area is cleared of threats?
5. What process do you use to collect evidence that belongs to citizens (e.g., cell phone video, cameras, security footage from private businesses, etc.)?
6. What process do you use to reunite personal items left at the scene with their owners?
7. Following this attack, what additional protective measures will your organization put in place at your organization or in your community?

### Scenario Update

### [Insert Month, Day, Year]

Several days later the investigation is still ongoing, but it appears that the suspect acted alone. Local businesses based in the impacted area are asking officials when they can reopen and resume normal operations. The [Insert county] Chamber of Commerce is asking what grants state and federal agencies can provide to help the city recover.

Many of the fatalities from the attack are local, and several families contacted the mayor’s office asking for police escorts for the funeral processions. They also asked what sort of city memorial events the local government plans to hold. National attention is focused on the community and the press is expected to try to cover the funerals and memorial services.

## Discussion Questions

1. Do you have any formal business continuity plans? If so, do they cover this type of incident?
   1. What are the short-term recovery objectives for your organization?
   2. What assistance would you look for from volunteer, community, or faith-based organizations?
   3. What would your organization do to support recovery in the community?
   4. What assistance would you expect from local, state, or federal agencies?
2. Are there plans for event cleanup in the case of this type of incident?
3. When would the area be deemed clear for use again?
4. What impact would the incident have on future events such as the fair?
   1. What outreach would your organization make to event sponsors and attendees?
5. Given the scenario, what measures would your organization need to support your employees following this event?
   1. How do you communicate this information to employees during the days following the incident?
   2. If some of your employees were killed or injured in the attack, how would this change your actions?
6. What resources are available to assist your organization with recovery?
   1. Has your organization pre-arranged agreements to obtain key resources following an incident?
   2. How would your organization manage victim donations following this incident?
      1. What plans exist, if any, to address donation management?
7. What types of information does your organization need restore of your critical infrastructure?
8. How can owners / operators and government officials prepare to handle public messaging / media in the aftermath of such an occurrence?
   1. Does your media plan include incidents such as this?
   2. How will you restore public confidence?
   3. Is your organization monitoring social media to maintain awareness of information spreading that may not be accurate?
      1. Who is responsible for this?
      2. What procedures exist to counter false information on social media?

# 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** | **Definition** |
| --- | --- |
| **AAR** | After-Action Report |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **EMS** | Emergency Medical Services |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **ICS** | Incident Command System |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **JIC** | Joint Information Center |
| **MAA** | Mutual Aid Agreement |
| **MAC** | Multi-Agency Coordination |
| **NIMS** | National Incident Management System |
| **NTAS** | National Terrorism Advisory System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SAR** | Suspicious Activity Reporting |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **TTX** | Tabletop Exercise |
| **UA** | Universal Adversary |
| **VIP** | Very Important Person |

