[Insert Cover Picture]

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

# Module One: Incident and Response

## Scenario

## [Insert Location]

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

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

At 2:31 p.m. on the second day of the fair, the [insert County] local law enforcement receives a credible bomb threat targeting the downtown building that houses the event headquarters and main art exhibit. Police begin evacuating the building and surrounding area and request the bomb squad. A patron exiting the main hall informs an officer he found an unattended black backpack that appears to have wires sticking out of it inside the entrance to the main art exhibit hall. Evacuating fair attendees spill out of the building and into the neighboring streets, mixing with people attracted to the commotion. At 2:38 p.m., a man driving a large pickup truck crashes through the light barriers securing the streets into the historic downtown and plows into the gathering crowd. The truck collides with a fire hydrant and stops, leaving a swath of killed and injured people.

After the truck comes to a stop, there is a brief pause before the truck driver staggers out of the vehicle carrying a rifle and wearing a holstered handgun. He fires into the crowd and forces his way into the headquarters building. He continues to shoot people inside the building until responding officers confront him, at which time he neutralizes himself. The local bomb squad arrives and attempts to identify and, if required, render safe the suspected device.

## Discussion Questions

1. What plans exist to prevent or deter an attack at your event?
   1. What threats do you spend the most effort preventing?
   2. Who is responsible for the security plan?
   3. Do multiple agencies involve themselves in the planning process?
   4. What plans exist to deter / prevent an active shooter (e.g., barricades, traffic control)?
   5. What plans exist deter / prevent an active shooter (e.g., screening, security presence)?
2. How does management staff and train security for this event?
   1. Is law enforcement present?
   2. Which organizations contribute to the security of the event?
   3. What training programs exist for personnel? Who trains them?
   4. How does your organization train personnel to respond to a vehicle intrusion?
   5. How does your organization train personnel to respond to an active shooter?
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. What resources does the event / venue provide that would help with response?
   2. What law enforcement assets does the event / venue stage to respond?
   3. What emergency medical services (EMS) assets does the event / venue stage to respond?
   4. Are there volunteer organizations or other partner groups that would have resources that would participate in the immediate response?
5. What are your crowd control and evacuation procedures for an event of this type?
   1. What measures exist for crowd control under normal conditions?
   2. Has your organization established plans for a mass evacuation?
      1. Who is responsible for activating the evacuation procedures?
      2. Has your organization specified a rally point for evacuees?
      3. Would weather impact this location?
      4. Are there secondary and tertiary rally points in case the primary point is a part of the incident or evacuees overwhelm it?
   3. What plans or procedures exist to work with access and functional needs populations?
   4. What are the procedures for evacuating distinguished visitors, such as the governor or mayor?
      1. Is this a written procedure?
      2. Who is responsible for enacting these procedures?
      3. Does event management advise distinguished visitor of emergency procedures prior to the event?
   5. What agencies would staff and control an evacuation?
      1. What training has your organization done on these plans?
   6. Would the event management / venue take any accountability of the staff working at the event and, if so, how do they accomplish this?
6. What notification methods (e.g., alerts, emails, telecommunications, text messages, special tools) do event organizers use to send alert information?
   1. What protocols exist for alerting event staff to an incident?
   2. What protocols exist for notifying authorities to the incident? How does your organization notify any first responders already on-scene?
   3. What protocols exist for alerting event participants to an incident?
   4. What protocols exist for alerting partner organizations to an incident?
   5. Who is responsible for sending out the alerts or warnings?
   6. If the incident overwhelms the cell network, does that affect your warning procedures?
   7. Are there alternate alert methods?
   8. 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 incident command look like during this phase of the response?
   1. How does each relevant agency approach incident command, and what would it look like in the opening minutes of the incident?
   2. At what point would you expect it to formalize?
   3. When would you expect unified command to begin coming together?
   4. Are key agencies and event personnel familiar with the Incident Command System (ICS)?
   5. What are each organization’s priorities at this stage of the incident?
   6. Who would call in mutual aid, and at what point would you expect that?
8. How would law enforcement conduct the response?
   1. Which agencies would involve themselves?
   2. Which agency would have the lead?
   3. How would law enforcement respond to the reports of a vehicle intrusion attack?
   4. How would the response change when it becomes an active shooter situation?
   5. How would law enforcement deal with injured or critically wounded individuals who are close to the unidentified potential explosive device?
9. How would responders conduct the medical response?
   1. Which organizations and agencies would involve themselves?
   2. Which organization or agency would have the lead?
   3. Has your organization established a mass casualty plan for this event?
   4. At what point would responder inform the hospitals about the incident?
      1. 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?
      1. What challenges would the ongoing participant evacuation pose to medical personnel?
      2. What actions, if any, would EMS personnel be able to take while the shooter is still active?
      3. What are EMS agencies’ procedures regarding entry into a warm zone?
      4. Do your EMS agencies have protective gear and training for tactical entry?
10. What information or warnings is your organization releasing to the public?
    1. Who is responsible for the initial messaging?
    2. How quickly are you releasing the information?
    3. What methods are you using to distribute information?
    4. What should the content of the messaging be?
    5. Do you send targeted information to businesses or people in the impacted area?
    6. Are businesses or other organizations providing their own messaging to their employees?
       1. How do they obtain information?
       2. How do they distribute it?
       3. Who in these organizations is responsible for this communication?
       4. Has your organization pre-built templates for different incidents?
    7. When would responders activate a Joint Information Center (JIC)?
    8. How do the different agencies and organization coordinate messages before activating the JIC?
11. If your organization or agency received information of a potential threat prior to the event taking place, what mitigation procedures would have taken place?
    1. How would those mitigation procedures have influenced the response if the attack had still occurred?
    2. Do your agencies and organizations cross-train on various attack scenarios?
    3. How would you prevent or protect against this type of attack happening at one of your events, or an event in your community?
12. What are some key best practices in prevention, protection, and mitigation?

# Module Two: Sustained Response

## Scenario

## [Insert Location]

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

After responders render the suspected bomb safe, EMS personnel rush in to triage the wounded. The attack left [insert number] people killed and [insert number] people wounded, with [insert number] of those in critical condition. [Insert County] Fire and EMS have already called in their mutual aid partners from surrounding counties, and ambulances are arriving. Several off-duty medical personnel who were attending the fair are assisting EMS personnel on-scene, attending to the most seriously injured. In addition, [insert County] Police officers securing the scene have reported that several off-duty law enforcement officers from different parts of the state have come to offer their aid.

Local media outlets were on-scene covering the festival and are now capturing video of the carnage and interviewing victims or anyone involved in the response. These media personnel are now within the crime scene and law enforcement needs to move them to a safe or designated location. The mayor arranges for a media briefing later that afternoon.

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

Early in the evening, the governor calls to express his condolences and details what the state is doing to respond. Shortly thereafter, representatives of state and federal agencies begin to arrive on-scene. At the press conference, the mayor expresses his grief and outlines to reporters from across the Nation what steps the city is taking to manage the incident. Law enforcement does not yet know the motivation of the attacker, but a person at the scene of the shooting who knew the assailant gave his name to the media. The assailant is now the subject of national reporting.

## Discussion Questions

1. What command structure would responders set up for the incident and how would it evolve over the course of the afternoon and evening?
   1. Which agencies would involve themselves in unified command?
   2. At what point would responders stand up the emergency operations center (EOC)?
      1. What agencies and organizations would be in the EOC?
   3. In addition to unified command, which agencies would have their own command centers set up in other locations?
   4. How would the EOC interface with unified command (phones, radios, liaisons, etc.) and how would participants define their roles?
   5. Would responders stand up a multi-agency coordination (MAC) group and, if so, when?
      1. How would you define the role of a MAC group in a situation such as this?
      2. How would the MAC group coordinate and interface with other command and control structures?
   6. How would arriving mutual aid agencies integrate into the command structure and at which locations (unified command at scene, EOC, hospital, etc.)?
   7. What is the role of private sector stakeholders in this command structure?
      1. Have they trained on incident command procedures?
      2. Is there cross training with public agencies on the private sector’s incident priorities?
2. Does your organization (public or private) have mutual aid agreements in place with other organizations?
   1. Whom would you rely on and for what resources?
   2. Are these agreements formal or informal?
   3. Would the aid be automatic, or would your organization have to request it?
      1. If requested, whom would you contact and how would you do it?
      2. Do you have a backup contact and communication method in case you cannot use the primary?
   4. What are the financial considerations when enacting mutual aid agreements?
   5. What limitations do you foresee within your organization’s mutual aid agreements in the event of this incident (legal, procedural, equipment, etc.)?
3. 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?
   1. How do you communicate with first responders?
   2. What other private sector organizations would you communicate with?
   3. What communication methods would you use for coordinating with your private sector partners?
   4. Who in your organization is responsible for communication during an incident?
   5. If the incident overwhelms the cell network, does that affect your communication procedures?
   6. Are there alternate communication procedures?
   7. Do you use social media to communicate with the public? If so:
      1. At what point in the incident would your organization use social media to communicate with the public?
      2. Who in your organization would be responsible for this function during an incident?
4. What communication methods (e.g., alerts, emails, telecommunications, text messages, and special tools) do first responders use to share information with other responders?
   1. What communications methods do local first response agencies use to communicate with their local counterparts (i.e., how do police officers communicate with fire or medical personnel)?
   2. What communication methods do local first response agencies use to communicate with their respective mutual aid partners?
   3. Are these methods the same?
   4. How do multiple agencies from multiple jurisdiction coordinate communications when they are all on-scene? Who is responsible for this?
   5. How do you communicate with the private sector?
   6. If the incident overwhelms the cell network, does that affect your communication procedures?
   7. Are there alternate communication procedures?
   8. Do you use social media to communicate with the public? If so:
      1. At what point in the incident would this begin?
      2. Who in your organization would be responsible for this function during an incident?
5. Who is responsible for notifying state or federal agencies of 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, EOC, MAC group, etc.)?
6. What role do city and county governments play in this scenario?
   1. Who is responsible for informing the mayor, county commissioners, or other local elected officials?
   2. Has your organization 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?
   3. Is there a location (such as the EOC) where elected officials will know to go during an incident?
      1. If so, where is it?
   4. What support from first response agencies would the mayor or county commissioner expect in holding a press conference on the incident?
      1. What information would they need?
      2. Would the mayor or county commissioner expect department chiefs to attend the conference?
7. What are your organization’s information sharing responsibilities at this point in an incident?
   1. What formal information sharing processes would your organization use at this point?
   2. What resources would your organization use to disseminate information?
   3. Who would be responsible for messaging in your organization?
      1. Would you coordinate messaging with any other organizations? If so, how?
   4. How would you send information to your employees?
   5. How would you send information to your patrons or customers (if applicable)?
   6. Who is responsible for communicating information to family members of those killed or injured?
   7. Who is responsible for communicating information to businesses the incident potentially impacted?
   8. What are your communication goals?
8. Does your organization have a designated public information officer (PIO)? If so:
   1. Are protocols in place for addressing media inquiries?
   2. How does the PIO receive information about the incident?
   3. Do they have pre-built templates for use in different kinds of emergencies?
   4. Would your organization use social media during an incident?
9. Have responders established a JIC? If so, at what point in the incident did this happen?
   1. Where would responders locate the JIC?
   2. Which agencies would involve themselves?
   3. Is there an SOP for a JIC?
   4. Would agencies coordinate social media messaging?
   5. Is there a location where reporters know to gather when there is an incident?
10. Would responders set up mass care facilities, family assistance, or reunification centers?
    1. At what point in time would they do this?
    2. Which agencies involve themselves, and who is responsible for leading this aspect?
    3. What procedures exist to set up these centers?
    4. Which facilities would responders use for these centers?
    5. How do responders make victims and family members aware of the location?
    6. Which agency or person, if any, would be in charge?
11. What is your agency’s protocol for addressing self-dispatching responders?
    1. Does it differ if the self-dispatching responders offer help in the initial moments of the attack, as opposed to later in the incident?
    2. Is the protocol the same for self-dispatching law enforcement as it is for EMS?
12. If [insert appropriate decision-making agency / organization] declared this a terrorist incident, what impact would that have?
    1. How would that impact federal and state involvement?
    2. If [insert appropriate decision-making agency / organization] determined a terrorist organization backed the attacker (as opposed to a lone wolf drawing inspiration from a terrorist organization) what impact would that have?
13. What steps do responders need to take to ensure the area is cleared of threats?
14. What is the process to collect evidence that belongs to citizens (cell phone videos, cameras, security footage from private businesses, etc.)?
15. How does your organization reunite personal items left at the scene with their owners?
16. What are some of your agency’s best practices for response?
17. Following this attack, what additional protective measures will be put into place at your organization or in your community?
    1. How would your organization obtain information on protective measures?
    2. How would your organization share any relevant classified information?
    3. How does your organization share any relevant information within your critical infrastructure sector?
       1. How do you communicate information to other members of your sector or receive information from them?
       2. Do you know how to contact your Sector-Specific Agency (SSA)?
       3. Do you have a Homeland Security Information Network (HSIN) account?
       4. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?
    4. Do you know how to contact your CISA protective security advisor (PSA)?

This page is intentionally left blank.

# Module Three: Short-Term Recovery

## Scenario

## [Insert Location]

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

Several days later the investigation is still ongoing, but it is clear the suspect acted alone. All evidence points to this being the result of an emotional breakdown arising from a domestic situation.

Local businesses based in the impacted area are asking officials when they can reopen and resume normal operation. 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 have asked what sort of city memorial events the local government has planned. National attention is focused on the community and many expect the press to try to cover the funerals and memorial services.

## Discussion Questions

1. What is the community’s plan to recover?
   1. Is there a formal recovery plan and, if so, does it cover this type of incident?
   2. Will [insert your organization] hold a memorial event in the community, and which organizations would take the lead in organizing it?
   3. What assistance would you look for from volunteer, community, or faith-based organizations?
   4. What would your organization do to support recovery in the community?
   5. What assistance would city agencies provide to private sector organizations?
   6. What assistance would you request or expect from the state?
   7. What assistance would you request or expect from the federal government?
   8. Are there contracts in place to assist in the cleanup prior to reopening?
   9. Are there any additional measures that law enforcement would take to ensure the safety of the community or to reassure citizens?
      1. How would your organization resource these measures?
   10. Who makes the decision on when to reopen the area?
       1. How does that person communicate that decision to the public and the media?
   11. At what point would you consider the recovery complete?
2. What impact would the incidents have on an event such as the future fairs?
   1. Would event organizers hold the event again?
   2. Would sponsors continue to support the event? What outreach would your organization make to them?
   3. Will event organizers face liability issues from the attack?
   4. Does the event have insurance that would help with this type of incident?
3. Does your organization have a business continuity or rapid recovery plan?
   1. Does it include a crisis communications plan?
      1. What type of messaging will your organization send to employees, vendors, and customers? How will you do this?
      2. What training do employees receive regarding media relations and the release of sensitive information?
   2. What are the short-term recovery objectives for your organization?
   3. What are the implications of being unable to open or operate for a period of time?
      1. Given the scenario, how long would [insert your organization] require the incident area remain cordoned off for the investigation?
      2. What would the financial impact be on your organization if a similar incident and ensuing investigation closed your building?
      3. Would your business voluntarily close because of this incident even if it did not directly impact you?
   4. Can your organization move key operations to another location?
      1. If so, how long would this take?
   5. Do you have any insurance that would assist given this scenario?
      1. If this incident were declared terrorism, would this impact insurance?
   6. What training plans exist for the business continuity plan? Does your organization exercise these plans (other than today)?
4. Given the scenario, what measures would your organization need to support your employees following this event?
   1. How does your organization communicate this information to employees during the days following the incident?
   2. Will counseling be available for employees and family members?
   3. Would your organization grant leave or time off?
   4. If your organization must suspend operations for a length of time, is there financial assistance available to employees?
   5. Are there any additional security measures that you would put into place following this event?
   6. How do you reassure employees as to their safety on the job?
   7. If the attack killed or injured some of your employees, how would it change your actions?
      1. Is there assistance available for injured employees? If so, what kind (counseling, monetary, legal, etc.)?
      2. Is there assistance available for the families of those employees who were killed? If so, what kind (counseling, monetary, legal, etc.)?
      3. How would the loss of personnel impact your operations? What steps might be taken to adjust for or mitigate this?
5. What resources are available to assist your organization with recovery?
   1. Does your organization have existing pre-arranged agreements to obtain key resources?
   2. If so, how do you activate these agreements (i.e., what type of coordination and request process do the agreements require)?
6. What are your organization’s interdependencies?
   1. What stakeholders are dependent upon your organization and its services?
   2. Who are the key stakeholders or groups that your organization relies upon to help restore operations and assets?
   3. What public sector organizations / resources do private sector organizations rely on to help restore critical infrastructure assets?
   4. What private sector organizations / resources do public sector organizations rely on to help restore mission-essential functions?
   5. Do you have established contracts / agreements with the organizations that control / own these resources / services for priority services in an emergency?
   6. Who are the key mobilizers or champions (either individuals or functional roles) in your organization or community who you must engage for an effective recovery?
7. What types of information does your organization need to assist in restoration of your organization’s critical infrastructure?
   1. What information would your organization expect to receive? How does your organization expect to receive it and from whom?
   2. What information would your organization expect to provide? How would your organization expect to provide it and to whom?
8. How can owners / operators and government officials prepare to handle the public messaging / media in the aftermath of such an occurrence?
   1. Does your media plan include incidents such as this?
   2. What is the plan to handle the significant media attention from national and international outlets?
   3. How will you restore public confidence?
   4. How will you resolve potential misinformation?
   5. How will you respond to media requests (written notices, press conferences, interviews, etc.)?
   6. 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?
9. Are there best practices for recovery that you would like to share?

# 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 |
| **CTEP** | CISA Tabletop Exercise Package |
| **EMS** | Emergency Medical Services |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **HSIN** | Homeland Security Information Network |
| **HSIN** – **CI** | Homeland Security Information Network – Critical Infrastructure |
| **ICS** | Incident Command System |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **JIC** | Joint Information Center |
| **MAC** | Multi-Agency Coordination |
| **NIMS** | National Incident Management System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **SSA** | Sector-Specific Agency |
| **TTX** | Tabletop Exercise |

