[Insert Cover Picture]

Gaming Industry Tabletop Exercise

Situation Manual

[Insert Date]

\*[Insert Caveat]\*

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

This page is intentionally left blank.

# Exercise Agenda

| 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: Threat |
| 9:45 a.m. | 9:55 a.m. | Break |
| 9:55 a.m. | 10:55 a.m. | Module Two: Incident 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 / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Gaming Industry 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 * Intelligence and Information Sharing * Interdiction and Disruption * On-Scene Security, Protection, and Law Enforcement * Operational Communications * Operational Coordination * Physical Protective Measures * Situational Assessment |
| **Objectives** | 1. Examine the effectiveness of overall emergency plans and procedures in response to an active shooter / improvised explosive device (IED) incident using the Incident Command System. 2. Assess the existing methods of coordination and communication between public (federal, state, tribal, and local) and gaming sector partners during response to an incident. 3. Examine post-incident alert and communication procedures as well as evacuation procedures for guests and employees following an incident. 4. Identify and examine critical functions, business continuity, and recovery plans to include roles and responsibilities in short and long-term recovery efforts following an active shooter / IED incident. 5. [Insert additional exercise objectives as necessary]. |
| **Threat or Hazard** | Active Shooter / Complex Coordinated Attack (CCA) / IED |
| **Scenario** | An interactive, discussion-based exercise focused on an active shooter / IED incident on the gaming industry. The scenario consists of three modules: Threat, Incident Response, and Post-Incident Recovery. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix B.] |
| **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 the effectiveness of overall emergency plans and procedures in response to an active shooter / IED incident using the Incident Command System. | * Intelligence and Information Sharing * Interdiction and Disruption * On-Scene Security, Protection, and Law Enforcement * Operational Communications * Operational Coordination * Physical Protective Measures |
| Assess the existing methods of coordination and communication between public (federal, state, and local) and gaming sector partners during response to an incident. | * Intelligence and Information Sharing * Operational Communications * Operational Coordination * Situational Assessment |
| Examine post-incident alert and communication procedures as well as evacuation procedures for guests and employees following a incident. | * Intelligence and Information Sharing * Operational Communications * Operational Coordination * Physical Protective Measures |
| Identify and examine critical functions, business continuity, and recovery plans to include roles and responsibilities in short and long-term recovery efforts following an active shooter / IED incident. | * Economic Recovery * Operational Communications * Operational Coordination |
| [Insert additional objectives as needed] | * [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 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: Threat
* Module Two: Incident 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 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: Threat

## Scenario

## [Insert Location]

### [Insert Incident Date - 9 Days]: 2:00 p.m.

The [Insert International Police Department/Intelligence Agency], acting on overseas intelligence, conducted a raid on an apartment in [Insert City, Country]. While the suspected subject was able to escape through a disguised hole in the apartment that led to a utility room, [Insert International Partner/Intelligence Agency] agents did discover information potentially relating to multiple targets throughout the United States and [Insert Country]. Specifically, they found maps and global positioning system (GPS) coordinates of the [insert well-known casino locations, such as the Las Vegas Strip and Atlantic City Boardwalk] along with the surrounding areas.

Investigators also found what appear to be bomb-making materials along with these maps. It is the opinion of [Insert International Police Department/Intelligence Agency] that the suspect likely made IEDs and either took them as they fled or previously hid them off-site. [Insert International Police Department/Intelligence Agency] also found significant amounts of print and digital propaganda from known terrorist groups. [Insert International Police Department/Intelligence Agency] briefed the United States’ Federal Bureau of Investigation (FBI) on the intelligence they obtained during the raid.

In coordination with the FBI, the secretary of homeland security issued an “Elevated” Threat Alert through the National Terrorism Advisory System (NTAS), warning of a credible threat against the United States. At this time, there is no specific information that would warrant the release of an “Imminent” Threat Alert. **(See Appendix A.)**

## Discussion Questions

1. What is the process by which your organization would receive intelligence and protective measure information concerning an overseas threat?
   1. Is your organization familiar with and / or subscribed to NTAS alerts?
   2. What organizations would you communicate with (e.g., local law enforcement agencies, state resources, your joint terrorism task force [JTTF])?
   3. Does your organization maintain a relationship with your CISA Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?
   4. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?
2. What internal information sharing and dissemination processes does your organization currently use?
3. How does your organization triage the information you receive (e.g., formal reporting, rumors, social media) for further dissemination within your organization and to your personnel?
4. What resources does your organization use to disseminate information?
   1. What notification capabilities (e.g., alerts, emails, telecom, text messages, special tools) do you use to share information and communicate protective measures implementation?
   2. Are there technological barriers, legal considerations, or cultural and institutional sensitivities that might affect information sharing?
5. Given current and established information sharing procedures, what types of official information (immediate information versus analyzed information) are the most useful to your organization?
   1. Does your organization perform independent analysis on the information you’re provided? If so, describe the process?
6. If your organization receives information related to potential threats against your facilities and personnel, how would you communicate this information to the appropriate entities (local law enforcement agencies, your JTTF, your CISA PSA, etc.)?
7. If someone observes identified “suspicious behavior” at a gaming industry venue, how do the facilities report this information locally and within the Commercial Facilities Sector and gaming industry?
   1. Does your organization track trends of suspicious behaviors across the Commercial Facilities Sector and the gaming industry nationwide?
8. Given evidence of a credible threat to the Commercial Facilities Sector, does your organization review your emergency response plans (e.g., site security plans, emergency occupancy plans, emergency action plans, or other appropriate plans)?
9. What protective security measures or recommendations, if any, will you employ at your organization following this international attack?
   1. Do you coordinate protective measure implementation with any other organization within the Commercial Facilities Sector, or with government entities, such as law enforcement agencies and your CISA PSA?
   2. How do organizations within the Commercial Facilities Sector and gaming industry communicate security measures they have put in place back to the government?
   3. How useful are the information bulletins and advisories the Department of Homeland Security (DHS) provides that recommend protective measures (e.g., a Joint Intelligence Bulletin [JIB])?

# Module Two: Incident Response

## Scenario

## [Insert Location]

### [Insert Month, Day, Year]: 10:00 p.m.

Numerous patrons and staff of [Insert Casino and Hotel] call 911 reporting an active shooter. According to the chaotic calls from [Insert Casino and Hotel], there are at least three armed individuals who entered the property during peak operation hours and began firing into a panicked crowd of casino patrons causing casualties. Local law enforcement responds immediately. Security personnel at the casino begin lockdown and evacuation procedures and attempt to get in touch with incoming local law enforcement.

**10:30 p.m.**

Security personnel monitoring cameras while the incident continues to unfold notify law enforcement of a potential IED placed by one of the gunmen, stating that the individual opened the bag and appeared to be fidgeting with something inside. This information prompts the initial senior responding officer / incident commander to request bomb squad support. The special weapons and tactics (SWAT) team requests the staging location for the incident.

Heavy cell phone use begins to degrade the cell phone network, and 911 operators are receiving many reports regarding the active shooters and an increasing number of suspicious package reports, particularly from callers claiming to be patrons of the [Insert Casino and Hotel] or in the area surrounding it. Both foot and vehicle traffic have greatly increased in the area, causing choke points that hinder both victims and emergency vehicles.

Local law enforcement arrives on-site and are currently inside the building attempting to locate the gunmen. After making entry, officers report that at least two dozen people appear to be injured or dead in their immediate vicinity.

Paramedics and other emergency medical personnel are also at the scene waiting for clearance to enter the facility and begin triage and transport of the victims. [Insert local hospital] is currently preparing for a mass casualty incident.

**11:10 p.m.**

Law enforcement reports that three gunmen have barricaded themselves inside a conference room and have as many as twelve hostages. During their entry, officers reported several suspicious packages. The [insert local law enforcement] bomb squad is actively investigating four suspicious packages, though fleeing patrons have dropped numerous bags, complicating the investigation and identification of potential IEDs. Emergency medical personnel and SWAT medics have begun extricating the victims from the casino and conducting triage and transport efforts to nearby medical facilities.

Hundreds of citizens and tourists have ignored law enforcement’s requests to disperse and continue gathering on the periphery of the security cordon in an attempt to observe the situation and see the progress of response. Local media teams have arrived at the frontlines of the scene and have begun broadcasting live reports and interviewing several hysterical witnesses.

**Discussion Questions**

1. What are your plans and procedures for responding to an active shooter?
   1. How does your security team interface with law enforcement responding to the active shooter?
      1. Does this interaction change for addressing a bomb threat?
      2. Does this interaction change for addressing a hostage situation?
2. What procedures do you use to address the credible threat of a bomb on the premises?
   1. How does the presence of an active shooter impact these procedures?
   2. Does your organization employ or contract with explosives detection canine teams?
      1. If so, how would the explosive detection canine teams be used during this incident?
3. Do you have a hostage protocol?
4. What resources or information do you expect law enforcement to need from the establishment to assist in responding to these threats?
5. What will your organization do to ensure the safety of first responders?
6. How will you establish and maintain site security?
   1. What assets would security have on hand (guards, cameras, etc.)?
   2. Are there specific procedures for security, or does a more general emergency response plan address the actions of security guards?
   3. What are the priorities of security?
   4. With whom is your organization’s security communicating?
      1. Who is responsible for contacting local responders?
      2. Who in your facility are you notifying, and who is responsible for this?
      3. What systems do you use to communicate with first responders (in-person, radio, 911 / dispatch, etc.)?
      4. Has your organization’s security cross-trained with local first responders in responding to an incident?
7. How would you coordinate an evacuation of your facility?
   1. Who makes the decision to evacuate or shelter-in-place?
   2. How does your organization communicate this decision?
   3. Have you pre-designated a rally point?
   4. Do you search or sweep the rally point before evacuating?
   5. Have your employees trained and drilled in either evacuation or shelter-in-place responses?
8. How would your organization assist the evacuation of patrons with access or functional needs?
9. What are the immediate resource needs and concerns facing the response? Where will you get them, and who will work to track them?
10. What are your organization’s information sharing responsibilities during the response to the incident?
    1. How would your organization access security camera footage during an incident? How can law enforcement access that footage?
11. What formal information sharing processes would your organization use at this point?
12. Do your organization’s emergency response plans (e.g., site security plans, emergency occupancy plans, emergency action plans, or other appropriate plans) contain protocols for properly responding to the incidents described in this module?
13. What resources does your organization use to disseminate information?
    1. What notification capabilities (e.g., alerts, emails, telecom, text messages, special tools) do you use to share information and communicate protective measures implementation?
    2. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing, such as religious customs that prohibit use of electronic communication during specific times?
       1. If so, how will you distribute threat-based alerts and notifications to community members who follow religious customs that prohibit use of electronic communication during specific times?
14. How does emergency response personnel gain access throughout the facility?
    1. Upon arrival of law enforcement, is there a “go bag” available to them containing desired items such as floor plans, access swipe cards, elevator keys, etc.?
15. How will responding personnel from emergency medical services (EMS) organizations, SWAT medics, law enforcement, and fire agencies coordinate and form an integrated rescue task force?
    1. Who will be in charge of this coordination?
    2. How will the rescue task force integrate into Unified Command?
16. How will local hospitals and medical facilities communicate and coordinate with the integrated rescue task force and other responding EMS personnel?
    1. Who will be the primary POC at the local hospital or medical facility?
17. How do you train your employees to act in the event of an active shooter?
    1. What formal training, if any, do you require?
    2. How does your organization train your security force to respond?
18. How does your organization alert employees to an incident?
    1. What about local and state law enforcement?
    2. What emergency communications plans currently exist?
19. How does your organization conduct an accountability check of your employees?
    1. Who is responsible for this? Who collects the information?
    2. What is done if an employee does not respond?
    3. Do your plans and procedures outline this?
20. What are the private sector’s emergency response priorities to this incident?
21. What type of command structure would responders 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. Have private sector stakeholders been trained on Incident Command procedures?
    4. Is there cross-training between local responders and the private sector?
22. Did responders activate the Emergency Operations Center (EOC)?
    1. If so, who would staff the EOC in this incident?
23. How do local, state, and federal agencies coordinate response operations?
    1. Who is responsible for this coordination?
24. Do you have pre-identified public information officers (PIOs)?
    1. Has your organization trained them for such incidents?
    2. Have your PIOs ever had the opportunity to work with local first responder and the jurisdiction’s PIOs?
    3. How do PIOs integrate into the command structure?
    4. In addition to what your organization is doing for public messaging, would other organizations be providing public information?
       1. Realistically, when would your organization address public information?
       2. What would your organization’s public information priorities be following an incident?
       3. Are there plans to coordinate public information between your organization, first responders, and other public and private partners?

## Scenario Update

## Location

### 11:20 p.m.

Officers are reporting that one of the assailants separated from the others and engaged law enforcement. [Insert law enforcement agency] officers were able to apprehend the individual. The bomb squad determined that two of the suspicious packages found at [insert facility] were IEDs and have rendered the devices safe. The incident commander is reporting that responders cleared the lobby and gaming areas of [insert facility] from potential IEDs and any active threats.

Several national outlets have begun on-scene news reporting. Reporters are interviewing those who were in [insert facility] when the attacks took place in addition to gathering as much information as possible from response and emergency management officials. The story is rapidly becoming headline news all over the United States.

### 11:30 p.m.

Law enforcement officers at [insert facility] report that they are hearing gunshots from the room in which the suspects are holding the hostages. They quickly breech the room and engage the two remaining gunmen. Moments later, officers report that they neutralized both of the remaining gunmen; however, one of the officers and one of the hostages also appear to be critically injured.

### [Insert Incident Date + 1 Day]: 1:10 a.m.

Working with [insert facility] security personnel and bomb technicians, law enforcement sweeps the building for additional gunmen and IEDs. Emergency medical operations continue in earnest. FBI agents work with state and local law enforcement officials to coordinate the upcoming investigation.

**Discussion Questions**

1. Following this event, what measures would other members of the gaming industry put in place?
2. What measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased patrols, etc.)?
3. Who is responsible for coordinating the risk communications message for your organization?
   1. Do you have an established media plan?
   2. What public relations steps are you taking to reassure potential patrons and return to normal business operations?
4. Who are the affected stakeholders?
   1. What decisions related to natural, economic, and infrastructure resources, if any, does your organization need to coordinate with affected stakeholders?
   2. What are the key messages that your organization is sharing concerning the continuing threat to your organization and stakeholders?
      1. Does your organization coordinate the message within the Commercial Facilities Sector and gaming industry?
      2. If so, what is the process for coordinating this message?
5. How are you communicating this incident with nearby businesses?
   1. What procedures does your organization have in place regarding coordination with local businesses?
   2. Who is responsible for implementing these measures?
6. What information do businesses in the area surrounding the incident expect to receive at this time?
   1. Who are the POCs from each organization who are responsible for sharing information following an incident?
7. How would this incident impact the operations of nearby businesses?
8. Would your organization review your emergency response plans (e.g., site security plans, emergency occupancy plans, emergency action plans, or other appropriate plans) after completing the response to these incidents?
   1. Who in your organization is responsible for reviewing these plans, if anyone?
   2. Who in your organization is responsible for activating these plans, if anyone?

# Module Three: Short-Term Recovery

## Scenario

## [Insert Location]

### [Insert Incident + 48 Hours]: 10:00 p.m.

The investigation at [Insert Casino and Hotel] is ongoing, and parts of the facility remain an active crime scene. Repairs and cleaning efforts are underway in other parts of the facility as the casino remains closed to guests. Many guests and employees are suffering from physical and psychological trauma, and news networks continue providing round-the-clock coverage of the attack and unfolding story.

The media are pressing for [Insert Casino and Hotel]and law enforcement officials to provide official statements. Additionally, social media is overrun with videos and pictures from the attack. Survivors and the public are demanding answers regarding publicly perceived lackluster preventive measures.

An investigation is still underway to determine the perpetrators and their motives, but law enforcement agencies state they will release the information once they confirm it.

**Discussion Questions**

1. How would your organization’s protective security measures change following this attack?
   1. Do you coordinate protective measure implementation with any other organization within the Commercial Facilities Sector and gaming industry? Or with government entities, such as law enforcement agencies and your CISA PSA?
   2. How does the Commercial Facilities Sector and gaming industry communicate the protective security measures they have put in place back to the government?
   3. How useful are the information bulletins and advisories DHS provides that recommend protective measures (e.g., a JIB)?
2. Who in your organization would contact law enforcement to determine the status of the investigation?
   1. Who determines when it is safe for employees / visitors to return to steady operations?
   2. How do you communicate this to the public?
   3. How would your organization encourage employees / visitors to return after such an incident?
3. What is the financial impact on your organization during the time it is closed?
4. What are your immediate goals in the recovery process? What do you see as your greatest challenges?
5. How is your organization addressing the issue of employees who refuse to come back to work because of security concerns?
6. How will your organization support patrons who need to evacuate the [Insert Casino and Hotel] and may not have immediately available housing options?
   1. Do you have intentions to reimburse patrons who had their reservations canceled because of the attack?
7. How would your organization handle the media in the aftermath of such an occurrence?
   1. Who is responsible for speaking to the media?
8. How would your organization handle social media in the aftermath of type of incident?
   1. What measures is your organization taking to disrupt the distribution of fake and / or erroneous information circulating on social media?
9. What local, state, tribal, and / or federal resources would your organization request?
10. What information sharing mechanisms are in place that could be relevant for an incident such as this?
    1. What communication structures are in place between your organization and local authorities?
11. How is your organization managing potential impacts to your brand and / or reputation?
12. What measures is your organization considering for protecting against similar attacks in the future?
13. How does this attack change your organization’s security posture?
14. What long-term mental health or behavioral counseling programs are available to employees and visitors still dealing with the psychological aftermath of the incident?
15. What protections exist to shield your organization from litigation after an incident?
16. What additional recovery issues is your organization considering at this time?

## Scenario Update

## [Insert Location]

### [Inert Incident + 5 weeks]: 6:30 p.m.

The investigation is officially closed, and law enforcement deemed the group, Universal Adversary (UA), responsible for the attack. The facility continues moving forward with cleanup efforts.

Mainstream media coverage and social media activity has dwindled. The casino and hotel remain closed until further notice.

**Discussion Questions**

1. For how long would you expect your facility to be shut down following such an incident?
   1. How would this impact your organization and employees?
   2. What is the protocol, if any, for personnel management following such an incident?
      1. Who is responsible for managing this?
   3. What safety requirements does your organization need to meet prior to re-opening the facility?
   4. How would you communicate with employees following the facility’s closure?
   5. How long can your organization remain closed while dealing with this incident?
   6. What is the financial impact on your organization during the time it is closed?
2. Following such an incident, what organizational and / or security changes would you make?
   1. Would you establish any additional security measures? What would they be?
3. What are your protocols for regular vulnerability assessments?
   1. Following the incident, would you re-examine them?
4. Is there a business continuity, continuity of operations, or rapid recovery plan that addresses this type of incident?
   1. Are there any potential liability issues from this incident that facility managers would be addressing at this point?
   2. What resources is your organization considering to assist in short-term recovery?
5. Would your organization update your emergency response plans (e.g., site security plans, emergency occupancy plans, emergency action plans, or other appropriate plans) after completing the response to these incidents?
   1. Who in your organization is responsible for updating these plans, if anyone?
6. What are your information sharing guidelines? What information, if any, about this incident would your organization share with other facilities in your sector?

This page is intentionally left blank.

# Appendix A: Sample NTAS Alert

This image is a sample National Terrorism Advisory System alert. 

This sample is blank and allows users to insert text with appropriate threat information. 

The sample also includes some pre-filled information that reads: 

DURATION: This bulletin will expire on or before [insert date] at [insert time] EDT. 

TYPES OF ADVISORIES: 
Bulletin: Describes current development or general trends regarding threats of terrorism. 

Elevated Alert: Warns of a credible terrorism threat against the United States. 

Imminent Alert: Warns of a credible, specific, and impending terrorism threat against the United States. 

HOW YOU CAN HELP: 
Report suspicious activity to local law enforcement who are best to offer specific details on terroristic indicators 

Report suspicious activity or information about threat, including online activity, to fusion centers and the FBI's Field Offices - part of the Nationwide Suspicious Activity Reporting Initiative. 

Learn how to recognize signs of pre-operational planning associated with terrorism or other criminal activity. 

BE PREPARED: 
Be responsible for your personal safety. Know where emergency exits and security personnel are located. Carry emergency contact and special needs information with you. 

Connect, plan, train, and report to prepare businesses and employees. Security resources can be accessed through the DHS's Hometown Security Campaign. 

STAY INFORMED: 

The U.S. Government will provide additional information about any emerging threat as additional information is identified.  The public is encouraged to listen to local enforcement and public safety officials.

This page is intentionally left blank.

# Appendix B: 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 is intentionally left blank.

# Appendix C: Relevant Plans

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

This page is intentionally left blank.

# Appendix D: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **CCA** | Complex Coordinated Attack |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **DHS** | Department of Homeland Security |
| **EMS** | Emergency Medical Services |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **FBI** | Federal Bureau of Investigation |
| **GPS** | Global Positioning System |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **JIB** | Joint Intelligence Bulletin |
| **JTTF** | Joint Terrorism Task Force |
| **NTAS** | National Terrorism Advisory System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **SWAT** | Special Weapons and Tactics |
| **TTX** | Tabletop Exercise |
| **UA** | Universal Adversary |

