**<Insert Cover Photo>**

**House of Worship Active Shooter**

**CISA Tabletop Exercise Package**

**Situation Manual**

**<Sponsoring Organization>**

## <Month, Day, Year>

## Cybersecurity and Infrastructure Security Agency

Updated September 2024

Table of Contents

[Exercise Agenda 3](#_Toc177975278)

[Exercise Overview 4](#_Toc177975279)

[General Information 6](#_Toc177975280)

[Module 1: Pre-Incident Information Sharing 8](#_Toc177975281)

[Module 2: Incident Response 9](#_Toc177975282)

[Module 2: Scenario Update 11](#_Toc177975283)

[Module 3: Recovery 13](#_Toc177975284)

[Module 3: Scenario Update 14](#_Toc177975285)

[Appendix A: Exercise Participants A-1](#_Toc177975286)

[Appendix B: Relevant Plans B-1](#_Toc177975287)

[Appendix C: Acronyms C-1](#_Toc177975288)

# Exercise Agenda

|  |  |
| --- | --- |
| Time | Activity |
| 20 Minutes | Introductions and Opening Remarks |
| 60 Minutes | Module 1: Pre-Incident Information Sharing |
| 20 Minutes | Break |
| 60 Minutes | Module 2: Incident Response |
| 2O Minutes | Break |
| 60 Minutes | Module 2: Scenario Update |
| 20 Minutes | Break |
| 60 Minutes | Module 3: Recovery |
| 30 Minutes | Hotwash and Closing Remarks |

*All times are approximate.*

# Exercise Overview

|  |  |
| --- | --- |
| Exercise Name | House of Worship Active Shooter Tabletop Exercise |
| Exercise Date(s), Time, and Location | <Exercise Date(s)>  <Time (e.g., 9:00 a.m. – 12:00 p.m.)>  <Exercise Location> |
| Purpose | Assess the resilience of <organization name> and their ability to respond to a significant threat. |
| Mission Area(s) | Prevention, Protection, Mitigation, Response, and Recovery [Select as appropriate based on the discussion questions chosen.] |
| Core Capabilities | * Community Resilience * Economic Recovery * Intelligence and Information Sharing * On-Scene Security, Protection, and Law Enforcement * Operational Communications * Operational Coordination * Planning * Public Information and Warning * Situational Assessment   [modify as needed] |
| Objectives | 1. Examine pre-incident intelligence and information sharing procedures between public and private sector stakeholders. 2. Examine response plans and procedures during an incident with a focus on:    * Incident Command System (ICS) / National Incident Management System (NIMS)    * Evacuation and shelter-in-place protocols    * Public messaging protocols    * Public Health, Healthcare, and Emergency Medical Services (EMS)    * Mass casualty incident (MCI) procedures    * Public / private sector coordination 3. Examine recovery and business continuity plans following an incident with a focus on:    * Family reunification    * Mental health and behavioral counseling    * Victim assistance   [Insert additional exercise objectives as necessary] |
| Threat or Hazard | Active Shooter |
| Scenario | Active shooter incident |
| Sponsor(s) | <Exercise Sponsor(s)> |
| Participating Organizations | Please see Appendix A for a complete list of participating organizations. |
| Points of Contact | |  |  | | --- | --- | | **<Organization POC(s)>**  Contact Information | **CISA Infrastructure Security Exercise Branch**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov) | |

# General Information

## Building Resilience

The purpose of the CISA Tabletop Exercise Packages (CTEPs) is to increase your organization’s resilience by assessing and validating capabilities and identifying areas for improvement.

## Participant Roles and Responsibilities

**Players** have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario.

**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.

**Facilitators** provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team (EPT) members may also assist with facilitation as subject matter experts during the exercise.

**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. [Remove for in-person exercises.]

**Data Collectors** are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

## Exercise Structure

This exercise is intended to be a facilitated exercise. Players will participate in the following:

* Scenario modules:
  + **Module** **1:** Pre-Incident Information Sharing
  + **Module** **2:** Incident Response
  + **Module** **3:** Recovery
* Hot Wash

***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired.*

## Exercise Guidelines

* This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
* Respond to the scenario using your knowledge of existing plans and capabilities, along with the valuable insights derived from your training.
* Decisions are not precedent-setting and may not reflect your organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
* There is no hidden agenda or trick questions. The resources and written materials provided are the basis for discussion.
* Issue identification is not as valuable as suggestions and recommended actions that could improve prevention, protection, mitigation, response, and recovery efforts. Problem-solving efforts should be the focus.
* In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

## Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions. 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 After-Action Report (AAR) / Improvement Plan (IP).

# Module 1: Pre-Incident Information Sharing

### <Incident Month, Day, Year: Time>

Over the last 6 months, there has been a notable increase in online threats and aggressive language directed towards [insert organization or faith group]. On [insert date], the regional [insert fusion / intelligence center] receives a report about an individual on an anonymous internet forum who has been making specific threats against [insert organization / faith / facility name]. Over the last few days, these threats have included detailed information about [insert organization / faith / facility name], specifically mentioning key staff members and community leaders.

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. How would your community / Faith-Based Organization (FBO) receive threat information?
   1. Who is that information communicated to?
   2. What kind of messaging, if any, would be released to your staff, volunteers, and community / organization members?
   3. Who is responsible for sharing the information?
   4. Under what circumstances is information shared amongst staff only?
      1. When is this information shared among members as a whole?
   5. How does your organization handle staff questions and concerns?
2. How might you become aware of open source threats against your community?
   1. How are your staff and community / organization members prepared to deal with specific threats?
3. What sort of training has staff gone through to recognize suspicious activity and potential threats?
   1. How often does this training occur?
4. How do staff report suspicious activity information, and who do they report this information to?
5. What additional security measures, if any, would your organization employ upon receiving a credible threat?
6. What security recommendations, if any, are local law enforcement making to your institution at this point?
7. How would reports of these types of threats impact the security posture or community gatherings at your facility?
8. What plans and systems are in place for your FBO to notify other faith communities of a potential threat if you receive suspicious or threatening messages?
   1. How often is your organization in communication with its security entity or other faith communities?
   2. Who is responsible for this communication?
9. What other internal or external notifications are made once a threat is reported?
10. How are staff and community / organization members expected to respond at this point?

# Module 2: Incident Response

### <Incident Month, Day, Year: Time>

During [insert religious service / event], an individual enters the back of [insert facility] with a firearm and begins shooting at people indiscriminately. Chaos erupts as people attempt to hide or flee the area while the shooter walks through the room, firing randomly.

Moments after the shooting starts, 911 operators receive calls describing the shooter, but reports differ regarding where the shooter is located within [insert facility].

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. What type of security, if any, does your organization have on-site?
   1. What sort of security screening procedures are in place, if any?
      1. What would be the immediate actions of security personnel?
      2. What are the priorities of your organization’s security / safety personnel?
   2. What technologies are in place to immediately contact local law enforcement? (i.e., panic button, Closed-Circuit Television (CCTV), etc.)
2. What Emergency Action Plan(s) (EAPs) does your organization have to address this type of threat?
   1. Who is responsible for drafting and reviewing emergency procedures?
   2. Do your plans include methods to alert/notify individuals onsite and offsite of the incident?
   3. How will individuals with sensory, intellectual, or cognitive disabilities; individuals with limited English proficiency; and others with access and functional needs be alerted to the incident?
3. Does your organization provide any sort of active threat training to staff and community members?
   1. What training resources from local, state, and federal partners has your organization utilized?
   2. What plan does your community have in place if community / organization members choose to intervene in the attack?
   3. What policies does your organization have directing certain individuals to take specific actions during an active shooter incident? Are there certain prohibited actions?
   4. What actions might they take to stop the shooter?
4. Who would be responsible for the initial communication with response authorities?
5. What are your evacuation and shelter-in-place procedures for an active shooter incident?
   1. How are staff and community / organization members trained and aware of these procedures?
   2. Who makes the decision whether to evacuate or shelter-in-place?
   3. How is this information communicated to staff and community / organization members?
   4. How have community / organization members been trained on identifying egress options within the facility?
6. What would law enforcement’s response look like at this stage?
   1. How is your organization communicating with law enforcement at this point?
7. If the facility has internal security and community / organization members that are armed, how do they avoid being viewed as a possible assailant by law enforcement?
8. How would your institution keep community / organization members calm and maintain order during the incident?
   1. What type of messaging would your organization plan to release at this point?

# Module 2: Scenario Update

### <Incident Month, Day, Year: Time>

Law enforcement arrives and neutralizes the assailant. Many individuals are still inside the building, and many call out for help for themselves and injured individuals around them. Friends and family members continue to call 911 centers requesting information on the status of their loved ones.

Bystanders crowd around the scene trying to determine what is happening. News and social media streams report on the event as the triage and transport of victims is underway. The attack results in [insert number and type of casualties] with children among the victims.

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. What incident command structure would be established upon law enforcement’s arrival?
   1. How would your organization take part in this structure?
2. What are the immediate concerns and responsibilities for your staff following an active shooter incident?
3. What plans does your organization have in place to lessen the impact of an active shooter incident?
4. What notification methods (e.g., alerts, emails, telecommunications, text messages, special tools) does your organization use to send alert information?
   1. How are you coordinating this message with responding agencies and media?
   2. Does your organization have a Public Information Officer (PIO) that could work with a Joint Information Center (JIC)?
   3. If your organization is part of a larger national organization, how would messaging be shared?
5. What would you communicate to your staff and community / organization members at this time?
6. How would your organization contribute to family reunification efforts?
   1. Does your organization or facility have a family reunification / assistance plan?
   2. Does your organization have accountability procedures, such as member rosters and procedures to track who is onsite during a given day or event?
      1. How often are such rosters updated?
   3. What resources would you expect from local and state response agencies to assist with reunification?
7. What plans exist for patient tracking?
   1. How would your organization collaborate with local hospitals to track patient transports?
8. What messaging are you sharing with the public at this point?
   1. Who on staff is responsible for coordinating and sending messaging to community members and media?
   2. Does your organization have pre-scripted messages or templates?
   3. How will your organization manage rumors and inaccurate information surrounding the incident?
9. How would your organization manage incoming calls and inquiries regarding the incident and their lost loved ones?
   1. Are there designated phone lines (or other mechanisms) and personnel identified for collecting and managing requests for information?
   2. What messaging would be provided in response to media inquiries?
10. What state and federal assistance would you expect or need at this point?

# Module 3: Recovery

### <Incident Month, Day, Year: Time>

[Insert number] hours have passed since the fatal event at [insert facility / event]. Family, friends, and community / organization members arrive on scene to search for loved ones. Many who were affected by the incident exhibit signs of distress and need immediate mental health and grief counseling services. Law enforcement have secured the facility and restricted access to the crime scene.

As the investigation continues, community members bring security concerns to [insert organization] leadership regarding upcoming events and activities at the [insert facility].

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. What recovery procedures does your EAP include?
   1. Who is responsible for initiating your organization’s recovery plan?
2. What is your local jurisdiction’s capability for handling the medical needs of multiple trauma victims?
3. What are the recovery objectives for your community / organization?
4. What processes are in place to allow community / organization members to retrieve personal belongings left during evacuation?
   1. How are victims’ belongings collected and returned to family members?
      1. Who takes the lead in providing this function?
5. What are your organization’s policies and procedures for receiving and managing volunteers to assist with recovery efforts?
6. What are your organization’s policies and procedures for receiving and managing the receipt of donations in the aftermath of an incident?
7. What are your procedures for handling any damaged areas of the facility?
8. How and what type of messaging will be sent to staff and your community / organization members?
9. What messaging are you sharing with the public at this point?
10. What procedures do you have in place for halting or slowing delivery of services during the investigation?
    1. What alternate venues are available for the delivery of services during the investigation?
    2. What virtual means for providing faith services are at your organization’s disposal?
11. What measures would be needed to support your staff and community / organization members following this incident?
    1. How is information communicated to staff during the days following the incident?
12. What additional security measures would you enact following this incident?

# Module 3: Scenario Update

### <Incident Month, Day, Year: Time>

It has been [insert number of days] since the incident, and the initial investigation has concluded. The scene is processed and released to the managers of [insert facility name] for further recovery efforts.

Untrue conspiracy theories and conflicting information has emerged on social media platforms, and leaders fear potential copycat attacks in other communities. [Insert facility] leaders are intent on ensuring this type of incident never happens again and begin searching for future preventive measures. Family and community members ask about memorial services for the deceased. Several community-initiated memorial sites have started and are growing.

### Discussion Questions

*The following questions are designed to help Players engage in discussions regarding your operational response to the scenario. These questions may not be a definitive list of concerns to address, nor is it required to address every question. The questions may be altered, removed, or added to as desired.*

1. What requirements must the facility meet to determine it is safe for reentry?
   1. How long would it take to assess the facility?
   2. What can be done to assess the facility while law enforcement is still in control of the scene?
2. What local, state, or federal resources are available to assist in recovery?
3. What are the implications of being unable to provide faith services during this period?
   1. What sort of financial impact would there be to your institution, if any?
4. What memoranda of understanding (MOUs) with other jurisdictions or businesses exist that could benefit your community / organization after an incident?
5. Who makes the decision on when the facility will reopen?
   1. How is that information communicated to the public and the media?
6. How do you assure staff and your community / organization members as to the safety of the facility?
   1. What sort of specific assurances would be put in place to ensure community / organization members that proper measures have been taken to handle an active shooter incident in the future?
7. What sort of mental health services can your organization make available to your staff?
   1. How would available services be communicated?
   2. Are there resources available to non-staff members who may have been attending services during the incident?
   3. What would your organization do if some staff and community / organization members are unable or unwilling to return to the facility because of physical or psychological trauma?
8. What special considerations for memorial services would need to be considered for victims from within this community / organization?
   1. Does your organization have a pre-identified area for establishing a memorial site?
   2. How would your organization manage impromptu memorial sites initiated by community members, and how would you communicate the proper areas?
   3. What plans are in place to deal with memorializing members of this community / organization?

# Appendix A: Exercise Participants

|  |
| --- |
| Participating Private Sector Organizations |
|  |
|  |
|  |
|  |

|  |
| --- |
| Participating Local Organizations |
|  |
|  |
|  |
|  |

|  |
| --- |
| Participating State Organizations |
|  |
|  |
|  |
|  |

|  |
| --- |
| Participating Federal Organizations |
|  |
|  |
|  |
|  |

|  |
| --- |
| Other Participating Organizations |
|  |
|  |
|  |
|  |

# Appendix B: Relevant Plans

*Insert excerpts from relevant plans, policies, or procedures to be discussed during the exercise. Materials may include:*

* *Organizational Standard Operating Procedures*
* *Training or employee onboarding protocols*
* *Facility or community maps*
* *Emergency contact information of key organizations*

# Appendix C: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| AAR | After-Action Report |
| CCTV | Closed-Circuit Television |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CTEP | CISA Tabletop Exercise Package |
| EAP | Emergency Action Plan |
| EMS | Emergency Medical Services |
| EPT | Exercise Planning Team |
| FBO | Faith-Based Organization |
| ICS | Incident Command System |
| IP | Improvement Plan |
| JIC | Joint Information Center |
| MCI | Mass Casualty Incident |
| MOU | Memorandum of Understanding |
| NIMS | National Incident Management System |
| PIO | Public Information Officer |
| POC | Point of Contact |
| SitMan | Situation Manual |
| TTX | Tabletop Exercise |