

Dams Sector Active Shooter 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 |
| --- | --- | --- |
| 8:00 a.m. | 8:30 a.m. | Registration |
| 8:30 a.m. | 8:45 a.m. | Welcome and Introductions |
| 8:45 a.m. | 9:50 a.m. | Module One: Initial Response Phase |
| 9:50 a.m. | 10:00 a.m. | Break |
| 10:00 a.m. | 10:55 a.m. | Module Two: Tactical Response Phase |
| 10:55 a.m. | 11:05 a.m. | Break |
| 11:05 a.m. | 12:00 p.m. | Module Three: Assessment Phase |
| 12:00 p.m. | 12:25 p.m. | Hot Wash |
| 12:25 p.m. | 12:30 p.m. | Closing Comments |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Dams Sector Active Shooter 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] at [insert exercise location]. Exercise play is limited to [insert exercise parameters].This exercise was developed using materials created by the Cybersecurity and Infrastructure Security Agency (CISA) for a CISA Tabletop Exercise Package (CTEP). |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response, and Recovery [select Mission Areas] |
| **Capabilities** | Planning, Intelligence and Information Sharing, Risk Management for Protection Programs and Activities, Operational Coordination, Physical Protective Measures, Operational Communications, and Public Information and Warning |
| **Objectives** | 1. Assess the roles and effectiveness of coordination between public safety officials and dam owners / operators in reacting to an adversarial event in accordance with existing plans and standard operating procedures (e.g., security plans, emergency actions plans, emergency response plans, memoranda of agreement, memoranda of understanding).
2. Examine the effectiveness of overall emergency response procedures in a no-notice adversarial event regarding the Incident Command Structure and logistical coordination among on-scene authorities.
3. Examine and evaluate facility incident response plans (e.g., security plans, emergency action plans, emergency response plans, or other appropriate plans) used during an adversarial event.
4. Assess the methods and effectiveness of internal and external communications during an adversarial event in accordance with existing plans and standard operating procedures.
5. Identify and evaluate response, mitigation, and recovery actions associated with an adversarial event at the facility.
6. Review information and threat sharing procedures and challenges between owners / operators and federal, state, and local government agencies.
7. Identify gaps, redundancies, developmental activities, and best practices in standard procedures in response to an adversarial situation.
8. [Insert additional exercise objectives as necessary]
 |
| **Threat or Hazard** | Active Shooter |
| **Scenario** | An interactive, discussion-based exercise focused on an international and domestic adversarial threat incident. The scenario consists of three modules: Initial Response Phase, Tactical Response Phase, and the Assessment Phase. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being utilized, 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 POC (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

The following 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** |
| --- | --- |
| Assess the roles and effectiveness of coordination between public safety officials and dam owners / operators in reacting to an adversarial event in accordance with existing plans and standard operating procedures (e.g., security plans, emergency actions plans, emergency response plans, memoranda of agreement, memoranda of understanding). | * Operational Coordination
* Operational Communications
* Planning
* Intelligence and Information Sharing
 |
| Examine the effectiveness of overall emergency response procedures in a no-notice adversarial event regarding the Incident Command Structure and logistical coordination among on-scene authorities. | * Operational Coordination
* Operational Communications
* Planning
 |
| Examine and evaluate facility incident response plans (e.g., security plans, emergency actions, plans, emergency response plans, or other appropriate plans) used during an adversarial event. | * Planning
* Risk Management for Protection Programs and Activities
 |
| Assess the methods and effectiveness of internal and external communications during an adversarial event in accordance with existing plans and standard operating procedures. | * Operational Communications
* Operational Coordination
* Public Information and Warning
 |
| Identify and evaluate response, mitigation, and recovery actions associated with an adversarial event at the facility. | * Planning
* Risk Management for Protection Programs and Activities
* Physical Protective Measures
 |
| Review Information and threat sharing procedures and challenges between owners / operators and federal, state, and local government agencies. | * Operational Communications
* Public Information and Warning
* Planning
* Intelligence and Information Sharing
 |
| Identify gaps, redundancies, developmental activities, and best practices in standard procedures in response to an adversarial threat situation. | * Planning
* Risk Management for Protection Programs and Activities.
 |
| [Insert additional objectives as necessary] | * [Insert additional capabilities as necessary]
 |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

* **Players:** 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:** 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:** Provides situation updates and moderate 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:** 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: Initial Response Phase
* Module Two: Tactical Response Phase
* Module Three: Assessment Phase

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: Initial Response Phase

## Scenario

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

### [Insert Facility Name and Location]

At 9:02 a.m., the local 911 operator receives a telephone call from a concerned citizen at [insert facility]. Amid audible gunshots, the frantic caller reports there is a man with what appears to be a gun in the parking lot of the facility and one injured victim in the parking lot. The caller also reports that the apparent assailant seems to have removed a lanyard with access credentials from around the victim’s neck. The caller reports seeing the shooter quickly approaching the main facility entrance.

Shortly after receiving the telephone call from the distressed citizen, the local 911 center notifies local and state law enforcement of a potential active shooter incident occurring at the facility. Additionally, a message is broadcasted to all surrounding law enforcement agencies notifying them of the situation. The 911 center also contacts emergency medical services and subsequently attempts to communicate with the facility’s security personnel.

Within minutes, security informed all personnel of the active shooter event, including the operations manager for the facility. The local 911 center and facility security are receiving additional telephone calls from individuals hearing gunshots.

At 9:22 a.m., local law enforcement and emergency medical services arrive at the scene of the incident and request facility floor plans. The victim assaulted in the parking lot is formally declared deceased. Dam security notifies facility personnel that law enforcement arrived on-site.

## Discussion Questions

1. Do owners / operators have the necessary security capability to protect personnel and the facility during an incident while waiting for law enforcement to formally respond?
	1. Do facility incident response plans (e.g., security plans, emergency actions plans, emergency response plans, or other appropriate plans) contain protocol for properly responding to similar incidents described in the module?
	2. Have security personnel been trained to provide guidance to employees for this type of incident?
	3. Are employees trained for this type of emergency incident? Is emergency contact information made available to the call desk? Are there established procedures for sheltering-in-place versus evacuation?
	4. If your facility has security personnel, are they clearly identifiable upon arrival of law enforcement?
	5. Do owners / operators have notification systems in place to warn employees located both on- and off-site during such an incident?
	6. What instructions will be given to the employees (e.g., evacuation, shelter-in-place, lockdown, etc.)?
2. Does your facility maintain security technology that can assist law enforcement in response efforts?
	1. Can security personnel assist in locating victims and assailants via closed-circuit television or similar capabilities?
	2. Are there access control capabilities at the facility to facilitate entry of first responders, prevent entry of visitors or additional employees, and manage contractors onsite?
	3. Does the facility have the ability to remotely control access to critical components or activate / deactivate card readers, including the capability to deactivate a specific card? If so, who would have access to this capability?
	4. Is there appropriate emergency lighting capability at the facility to deal with a nighttime incident?
3. Do state and local officials effectively coordinate when responding to an incident at the facility?
	1. Are the necessary memorandums of understanding and memorandums of agreement in place for external jurisdictions to assist in response efforts?
	2. Does local, county, and state law enforcement have incident response plans (e.g., security plans, emergency actions plans, emergency response plans, or other appropriate plans) for an active shooter situation? If so, who leads the response?
	3. What would state and local officials need from owners / operators during an incident similar to that detailed in this module?
4. How is emergency response coordinated?
	1. Are any of the facility’s incident response plans (e.g., security plans, emergency actions plans, emergency response plans, or other appropriate plans) provided to first responders in preparation for potential incidents?
	2. Upon arrival of law enforcement, is there a “go bag” available to them containing desired items such as facility map / floor plans, access swipe cards, elevator keys, etc.?
	3. Are there any safety concerns that need to be addressed (e.g., entering restricted or hazardous areas)?
	4. How do emergency response personnel access the buildings?
	5. Have local law enforcement / first responders participated in exercises and / or training at the facility?
5. How are emergency communications handled?
	1. If critical telephone calls cannot get through, are alternate means of communication available?
	2. How will owners / operators interact with media representatives and control media access to the facility?
	3. Are there procedures in place to manage the media when they arrive?
	4. Should additional emergency announcements be made to the public?

This page is intentionally left blank.

# Module Two: Tactical Response Phase

## Scenario

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

**[Insert Facility Name and Location]**

Law enforcement officers on-site assemble a contact team and are granted access to the facility. To secure the facility, officers enter the building to search for the assailant and any other potential victims. Concurrently, other law enforcement officers establish a command post to direct responding personnel. Considerations are also being made to close nearby roads and request residents in the immediate area to shelter-in-place until the situation is contained.

At 9:24 a.m., additional gunshots are heard, and law enforcement officers direct facility personnel to a more secure location. Within minutes, reports from employees who fled the facility indicate that the assailant is heading toward the control room. Control room operators report hearing gunshots. Local news media arrive on the scene to document the incident. Additional emergency medical services and law enforcement officers also arrive at this time.

Law enforcement informs facility personnel that the assailant was neutralized at the entrance of the control room. Officers continue to conduct additional search and secure missions and begin evacuating employees.

## Discussion Questions

1. Do the facility’s incident response plans (e.g., security plans, emergency action plans, emergency response plans, or other appropriate plans) cover emergency coordination activities described in the modules?
	1. How is the response coordinated and who maintains decision-making authority when management is not available?
	2. Is delegation of authority captured in the security plan or any other plan?
	3. If doors to critical facility components are locked, how does law enforcement obtain access?
	4. Is there a safe location identified for people who are evacuating the immediate area?
	5. Have credentialing procedures been developed and coordinated with local / state law enforcement?
2. What are the specific local law enforcement policies and procedures regarding active shooter incidents?
	1. What personnel resources do you have available to handle the situation and establish a secure perimeter?
3. What elements of the National Incident Management System (NIMS) will be used in managing this situation?
4. Does the dam owner have a sufficient existing security capability to protect staff and the facility in an emergency?
	1. Is there a way to account for employees (i.e., those who reported for work that day versus those on leave)?
	2. How is media access to the facility and staging areas managed?
	3. What access control is or should be in place?
	4. Can the operators secure the control room?
	5. What are the procedures for safely securing any critical component or operation of the facility?
	6. What other life safety issues should be considered?
5. Does this facility have physical security measures that may be relevant to this scenario?
	1. What types of perimeter security does this facility have (e.g., fences, doors, gates)?
6. What types of vehicle control checkpoints are present (e.g., barriers, driveways, parking lots)? How does law enforcement determine that the scene is cleared and there are no additional shooters?
	1. Once an all clear is given, how is that information communicated to all personnel sheltered-in-place?
7. For a prolonged incident with a known assailant, law enforcement will need all available information on the assailant as soon as possible. Can that information be provided if law enforcement requests it?

# Module Three: Assessment Phase

## Scenario

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

**[Insert Facility Name and Location]**

At 9:40 a.m., law enforcement informs facility personnel that there are no additional assailants. Law enforcement also reports approximately four additional fatalities and seven wounded. Law enforcement announces that they are going to initiate a controlled employee evacuation for all remaining employees. At this time, the incident commander provides a statement to all personnel and the public informing them of the conclusion of the incident. Law enforcement deems the facility a crime scene until further notice.

Ten minutes later, emergency medical services enter the facility and report that there are currently five fatalities and seven wounded. The wounded are transported to a local hospital and the extent of their injuries is unknown at this time. This information is relayed to the facility’s emergency coordinator. Neighboring facilities are notified that the facility has been secured.

At 10:00 a.m., emergency medical services relay information to law enforcement and facility personnel that all seven gunshot victims are in critical condition. Law enforcement asks for help in identifying three of the injured individuals. The remaining four were identified through personal identification cards.

Over the next hour, the names of the five deceased victims, as well as the injured personnel, are provided to the dam owner and family notifications begin. Law enforcement is evacuating the facility on an area-by-area basis. Security personnel are excluded from this evacuation but will remain on-site to provide support as necessary.

At 11:50 a.m., the facility owner releases an official statement to the media about the incident.

## Discussion Questions

1. Do current security plans sufficiently address coordination of emergency response personnel?
	1. What does the facility emergency coordinator need to consider (e.g., casualties, evacuation routes, hospitals)?
	2. Are there pre-determined locations for a command post and staging area(s)?
	3. Is there a process to assist law enforcement with victim identification?
2. What information sharing mechanisms are in place that could be relevant for an incident such as the one described in this scenario?
	1. Would owners / operators be able to share information and pass pertinent information to prevent potential attack at other facilities?
	2. Would owners / operators be able to relay information to federal, state, and local authorities, including fusion centers?
	3. Would owners / operators be able to receive information from their federal, state, and local officials, including fusion centers?
	4. Would owners / operators share information with the families of employees to keep them apprised of the situation? If so, how?
3. How will personnel accountability and communication be coordinated?
	1. Who is responsible for making a list of evacuees?
	2. How do employees leave when the parking lot is a crime scene and cannot be accessed?
	3. How is information communicated with personnel and families during the days following the incident?
	4. Will counseling for employees and family members be available?
4. Are owners / operators prepared to handle the public messaging / media in the aftermath of such an occurrence? If so, how?
5. How will law enforcement coordinate the handling of the facility as an active crime scene?
	1. How will law enforcement communicate status with owners / operators?
	2. How will the facility function with this impediment?
	3. Can law enforcement estimate how long access will be restricted because the facility is a crime scene?
6. How will the ramifications of such an event be addressed regarding business continuity planning or rapid recovery operations?
	1. Does the facility have an established continuity of operations plans?
	2. Will owners / operators face liability issues?

# 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 |
| **EPT** | Exercise Planning Team |
| **HSIN** | Homeland Security Information Network |
| **IP** | Improvement Plan |
| **NGO** | Non-Governmental Organization |
| **NIMS** | National Incident Management System |
| **POC** | Point of Contact |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert |
| **TTX** | Tabletop Exercise  |

