Dams Sector Adversarial Threat 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:  |
| 9:50 a.m. | 10:00 a.m. | Break |
| 10:00 a.m. | 10:55 a.m. | Module Two:  |
| 10:55 a.m. | 11:05 a.m. | Break |
| 11:05 a.m. | 12:00 p.m. | Module Three:  |
| 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 Adversarial 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** | 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 when reacting to an adversarial event in accordance with existing plans and standard operating procedures (e.g., security plans, emergency action plans, emergency response plans, memoranda of agreement, memoranda of understanding, etc.).
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 operating procedures in response to an adversarial situation.
8. [Insert additional exercise objectives as necessary]
 |
| **Threat or Hazard** | Adversarial Attack (domestic and international). |
| **Scenario** | An interactive, discussion-based exercise focused on an international and domestic adversarial threat incident. The scenario consists of three modules: International Threat Period, Domestic Threat Period, and the Domestic Attack. |
| **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 when reacting to an adversarial event in accordance with existing plans and standard operating procedures (e.g., security plans, emergency action plans, emergency response plans, memoranda of agreement, memoranda of understanding, etc.). | * 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 action 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 operating procedures in response to an adversarial threat situation. | * Planning
* Risk Management for Protection Programs and Activities
 |
| [Insert additional objectives as necessary | * [Insert 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: International Threat Period
* Module Two: Domestic Threat Period
* Module Three: Domestic Attack

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: International Threat Period

## Scenario

## [Insert Location 1]

### [Insert Month, Day, Year]: 9:30 AM

At approximately 9:30 a.m. local time, as personnel at [Insert international dam name] Dam are carrying out their daily routine, two suspicious vehicles approach the main entrance gate. A security guard halts a decrepit pickup truck and an orange and white taxi. As the security guard approaches to challenge the vehicles, the driver of the pickup truck drives forward, striking the security guard and breaching an entrance to the perimeter barricade. Once inside the perimeter of the dam, two men emerge with rifles and engage the remaining security guards with small arms fire.

In the ensuing confusion, the taxi driver drives through the breach and directly into the dam control structure, detonating a vehicle-borne improvised explosive device (VBIED) upon impact. The explosion kills several personnel and seriously damages the structure of the dam, potentially leading to catastrophic failure. [Insert country 1] government officials quickly secure the area, evacuate survivors, and clear the immediate area of potential threats.

## [Insert Location 1]

While the attack on the [Insert location 1] Dam received virtually no international media attention, the U.S. Government, through relationships with its local liaisons and other intelligence collection capabilities, became aware of the incident at approximately 5:00 p.m. local time. In addition, an international terrorist group known as the “Universal Adversary” (UA) released a video on the internet claiming responsibility for a suicide operation against the [insert country 1] government in retaliation for its cooperation with the U.S. in conducting counterterrorism operations.

## [Insert Location 2]

### [8 Days After Events in Location 1]: 2:30 PM

During a quiet afternoon, a loud explosion occurs at an apartment building at 2:30 p.m. local time in the eastern [insert country 2] town of [insert town]. Local law enforcement and emergency medical services personnel respond to the scene and find one man deceased with another severely wounded. After putting out the flames, investigators discover suspicious materials and alert [insert country 2] government investigators to the scene. Upon closer examination, authorities discover that the suspects possessed information and data about the [insert dam name] Dam on the [insert river name] River, [insert country 2]’s most prominent dam, including maps and reconnaissance photos.

## [Insert Location 2]

### [Insert 2 Days After Events in Location 2]: 11:30 AM

At approximately 11:30 a.m. local time, after a thorough investigation and further analysis of the materials found at the explosion site, [insert country 2] authorities conclude that the men were part of a terror cell with links to the UA terrorist group responsible for the previous week’s attack in [insert country 1]. Investigation into the history of the deceased reveals that he had studied chemistry in the U.S. for a number of years on a student visa and maintained links to contacts in the U.S. [Insert country 2] authorities alert the U.S. Department of State and the Federal Bureau of Investigation (FBI) legal attaché in [insert city], [insert country 2]. Based on materials found in the apartment and the emerging evidence of a nexus of coordination between terrorist elements in the Caucuses and the U.S., FBI concludes that although the threat is nebulous and unspecific, the UA terror group is targeting the continental U.S. for attack.

## [Insert Location 3]

### [Insert 14 Days After Last Events in Location 2]: 10:30 PM

At approximately 10:30 p.m. local time, continuing a campaign against international terrorism and using intelligence gleaned from previous operations, specialized units of the [insert country 3] Army conduct a nighttime assault on a makeshift terrorist base in the northern [insert country 3] town of [insert town]. Catching the terrorists by surprise, the [insert country 3 people] overwhelm and kill the terrorists and take control of the location. Examination of the deceased terrorists reveals one of them is a known radicalized [insert country 4] citizen. [Insert country 3] authorities alert the [insert country 4] diplomatic representative in the capital city of [insert city].

## [Insert Location 4]

### [Insert 7 Days After Events in Location 3]: 10:30 AM

After the previous week’s discovery of a radicalized [insert country 4] citizen, [insert country 4] authorities initiate an investigation into the background and activities of the deceased [insert country 4] terrorist at 10:30 a.m. local time. The investigation reveals that the individual was part of a radicalized cell plotting to conduct terrorist attacks throughout the world and possibly in the U.S.

During one of a number of raids conducted throughout [insert city], [insert country 4], investigators discover that the suspects have had contact with associates in the U.S. and in some cases have traveled there themselves. As was the case in [insert country 2], [insert country 4] authorities discovered bomb making materials and plans to attack targets such as electrical generating stations, power plants, and dams.

Based on the potential link to the U.S., [insert country 4] authorities are quick to share information with FBI and U.S. Department of State representatives in [insert city]. FBI, analyzing the newly developed information in addition to what was previously known, determines that it is necessary to release a bulletin warning critical infrastructure owners / operators in the U.S. of the potential, but unspecific threat to facilities.

## Washington, D.C.

### [Insert 1 Day After Events in Location 4]: 9:00 AM

At 9:00 a.m. local time, based on the events of the preceding month, FBI, in conjunction with the Department of Homeland Security (DHS), releases a joint information bulletin to critical infrastructure owners / operators in sectors that the FBI believes may be at risk for terrorist activity, particularly Dams Sector stakeholders. Although unable to highlight specific targets or terrorist actions, the bulletin delivers a general warning that a credible, albeit non-specific, terror threat is present and prompts owners / operators to be alert and aware of activity around their facilities. While unable to mandate any specific action, the bulletin lists recommendations for increasing security measures.

## Discussion Questions

1. When the federal government issues a joint bulletin to owners / operators in the U.S., what protective measures will owners / operators undertake given the scenario at this point?
2. In what manner are owners / operators going to receive information passed from the federal government?
	1. Are owners / operators familiar with the Homeland Security Information Network (HSIN) portal?
	2. Is there effective coordination in place with state and local fusion centers?
	3. Do owners / operators have a strong working relationship with CISA Protective Security Advisors (PSAs)?
	4. Does a general warning, such as the bulletin in the above scenario, meet the information needs of owners / operators?
3. What is the level of communication between owners / operators in the Dams Sector?
	1. What mechanisms or methods are in place for owners / operators to share information and coordinate with one another?
	2. If one facility generates information that may be useful to the rest of the sector, will they share that information with their colleagues (e.g., via the Suspicious Activity Reporting [SAR] tool available on the HSIN Dams portal)?
4. Based on the scenario until this point, will owners / operators make any increased effort to coordinate with federal, state, and local government representatives?
	1. Do owners / operators believe there is an effective relationship in place with federal, state, and local government agencies to exchange information?
	2. What, if anything, do owners / operators expect from federal, state, and local authorities?
5. Based on the information presented in this module, will federal, state, and local authorities take any increased protective measures?
	1. What authority do federal, state, and local officials have over individual facilities in their jurisdictions?

This page is intentionally left blank.

# Module Two: Domestic Threat Period

## Scenario

## [Insert Facility Name and Location]

### [Insert 60 Days After the End of Module One]

At approximately 10:45 a.m. local time, a security guard stationed at the perimeter fence of the facility, notices for the second day in the past week that a vehicle approaches the fence, stops short, turns around, and drives back the way it came. Shortly after, the security guard observes a man from a distance emerge from the vehicle and make use of what appears to be binoculars. The security guard notes what information he can: make, model, and color of the vehicle and a general description of the individual. The security guard subsequently makes a telephone call to the local police to file a SAR.

At 11:30 a.m. local time, a local law enforcement officer dispatched to the facility makes contact with the security guard, takes a report, and speaks with other personnel. The [insert local police department] alerts its patrolling law enforcement officers to be on alert for the suspicious vehicle. However, follow up patrols of the area reveal no trace of the suspicious vehicle or individual.

At 3:30 p.m. local time, the responding [insert local police department] files a report with the state fusion center advising of possible suspicious activity in and around the dam. The report includes the narrative and description of the security guard’s observations earlier in the day. Analysts at the fusion center are concerned after seeing multiple reports of similar “probing” occurring at U.S. dams over the past three weeks.

## Discussion Questions

1. At this point, what, if anything, do owners / operators expect from federal, state, and local officials?
2. Will the fusion center disseminate information to owners / operators at this point?
	1. If the fusion center does disseminate a product, how will it reach owners / operators?
	2. Do owners / operators have a representative at the fusion center?
3. Given that relevant intelligence bulletins or reports regarding suspicious activities at dams have been disseminated through fusion centers, what specific security measures will the owners / operators take?
4. What memorandums of understanding / memorandums of agreement are established to support any security measures that would be implemented?
	1. Will additional resources be necessary to support increased security needs?
5. Does the facility have physical security measures that may be relevant to this scenario?
	1. Does the facility have vehicle barriers?
	2. Does the facility have security fencing and gates?
	3. Do buildings feature hardened security openings (e.g., doors, locks, windows, skylights, loading docks)?
	4. Are there controls for delivery vehicles? Are those who are admitted for approved services (e.g., letter carriers) identified and approved for admission?
	5. Are there security controls for parking areas?
	6. Is the facility open to the public? If so, are there access controls for visitors?
	7. Does the facility have access controls for employees?
	8. Does the facility have intrusion systems to detect unauthorized facility access?

# Module Three: Domestic Attack

## Scenario

## [Insert Facility Name and Location]

### [Insert 11 Days After the End of Module Two]

At approximately 12:45 p.m. local time, during the lunch hour of a routine, quiet day at the dam, an older sedan drives down the access road toward the personnel entrance gate. Following the sedan is an older van, approximately 200 meters behind. The security officer at the gate becomes immediately suspicious and advises his partner to radio the supervisor inside the facility. The lone driver exits the sedan, claims that he is having engine trouble, and walks towards the security station. As the security guard advises the man to stay back, he detonates a suicide vest, killing himself and the security guard.

The van, having maintained its distance from the sedan during the detonation, takes advantage of the situation and proceeds up to the gate, ramming the sedan through the barricade. When the van rolls to a stop, three men wearing military-style magazine vests and camping-style backpacks exit from its doors with assault rifles. In response to the initial explosion, additional security officers from inside the facility appear and begin to engage the assaulters with small arms fire. The high volume of fire from the assailants forces the security guards to seek cover. The attackers proceed toward the facility control room to commandeer operation of the facility.

Terrified from the explosion and echoes of gunfire outside the control room, personnel immediately secure the control room entrance. Personnel begin frantically calling 911 at 12:47 p.m. local time, and local law enforcement officers are dispatched immediately. Every available asset, including tactical and aviation teams from nearby municipalities, are directed to the facility.

At 12:57 p.m. local time, the first law enforcement officers arrive at the facility and establish a perimeter. Shouting and intermittent bursts of gunfire can be heard from within the facility. The 911 dispatchers advise responding units that there are employees barricaded inside the control room and that multiple, unidentified armed assailants are believed to be still alive and present at the facility. Initial law enforcement units are ordered to secure the perimeter and await the arrival of additional tactical teams.

At approximately 1:15 p.m. local time, local media have become aware of the major emergency occurring at the dam because of monitoring law enforcement and radio transmissions. Reporters are dispatched to the scene. National networks begin receiving reports of a major event and start covering the incident at the dam.

Local agency tactical teams arrive on the scene and establish a command post at approximately 1:22 p.m. local time. The sounds of shooting have quieted, and no movement can be observed from the perimeter fence. The 911 dispatch reports that personnel inside the control room are still barricaded and alive. Assailants are believed to be alive and present at the facility.

The newly arrived tactical teams quickly breach the perimeter and begin a coordinated clearing of the facility. Upon approaching the control room, the teams are engaged by two assailants concealed in an entryway. After a fierce but short exchange of gunfire, the tactical teams report that both assailants have been killed. Facility clearing continues. The 911 dispatch advises trapped staff to wait for tactical team entry. There are still no report of assailants inside the control room.

At 1:40 p.m., special agents from the nearest FBI field office arrive, check in with the command post, and begin preparations for post-incident crime scene investigation.

At approximately 2:07 p.m., tactical teams declare the facility secure. Trapped control room personnel are freed. The bodies of two assailants are located near the entryway. The third assailant is found a distance away, apparently dying from wounds sustained in the earlier engagement with security officers. The vicinity of the control building is littered with shell casings and discarded magazines. Paramedics rush in to treat the wounded and evacuate the deceased.

FBI assumes command of the scene and initiates a criminal investigation at 2:15 p.m. local time. The death toll includes three security officers, two facility personnel, and four assailants. Three additional personnel with serious wounds and one law enforcement officer with a non-life-threatening wound are also treated.

## Discussion Questions

1. What level of coordination do owners / operators have with local law enforcement?
	1. Would law enforcement officers responding to the scene of an emergency at a dam have access to critical information such as floor plans and layouts of the facility?
	2. Would emergency responders have difficulty obtaining physical access to the facility, keys, locks, etc.
	3. Have credentialing procedures been developed and coordinated with local / state law enforcement?
2. What elements of the National Incident Management System (NIMS) will be used in managing this situation?
3. Does the owner have the necessary security capability to protect personnel and the facility during an incident while waiting for law enforcement to arrive?
	1. Do existing incident response plans (e.g., security plans, emergency action plans, emergency response plans, or other appropriate plans) cover situations as described in this module?
4. What information sharing mechanisms are in place in the event of an incident?
	1. Would owners / operators be able to share pertinent information quickly to prevent potential attacks at other facilities?
	2. Would owners / operators be able to pass information to federal, state, and local authorities? If so, how would that be done?
	3. Would owners / operators be able to receive information from federal, state, and local officials? If so, how would that be done?
5. Is there effective coordination between federal, state, and local officials?
	1. Are the necessary memorandums of understanding and memorandums of agreement in place for one jurisdiction to assist another in the type of situation detailed in this module?
	2. What would federal, state, and local officials need from owners / operators during an incident similar to that detailed in this module?
	3. Would federal, state, and local authorities have sufficient resources to respond to such an attack without leaving nearby facilities unprotected?
6. How will the handling of public messaging / media relations occur?

This page is intentionally left blank.

# 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 |
| **DHS** | Department of Homeland Security |
| **EPT** | Exercise Planning Team |
| **FBI** | Federal Bureau of Investigation |
| **HSIN** | Homeland Security Information Network |
| **IP** | Improvement Plan |
| **NGO** | Non-Governmental Organization |
| **NIMS** | National Incident Management System |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SAR** | Suspicious Activity Reporting |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert |
| **TTX** | Tabletop Exercise  |
| **VBIED** | Vehicle-Borne Improvised Explosive Device |

