[Insert Cover Picture]

Water and Wastewater Sector 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 |
| --- | --- | --- |
| 8:30 a.m. | 9:00 a.m. | Registration |
| 9:00 a.m. | 9:15 a.m. | Welcome and Participant Briefing |
| 9:15 a.m. | 10:30 a.m. | Module One: Threat and Initial Incident |
| 10:30 a.m. | 10:45 a.m. | Break |
| 10:45 a.m. | 12:00 p.m. | Module Two: Incident and Incident Aftermath |
| 12:00 p.m. | 12:30 p.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Water and Wastewater Sector 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, and Response [select appropriate Mission Areas] |
| **Capabilities** | * Planning * Intelligence and Information Sharing * Risk Management for Protection Programs and Activities * Public Information and Warning * [insert other capabilities] |
| **Objectives** | 1. Review intelligence and information sharing and dissemination processes in relation to a credible threat to domestic critical infrastructure owners / operators. 2. Assess information sharing capabilities with the public; sector partners; and federal, state, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures. 3. Discuss private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under the National Incident Management System (NIMS) with local, state, and federal agencies. 4. [List exercise objectives] |
| **Threat or Hazard** | Cyberattack (domestic and international). |
| **Scenario** | The exercise begins with a series of cyber-attacks on water and wastewater systems overseas and a threat against similar systems in the United States. Following that, there are multiple cyber-attacks on domestic water and wastewater systems. |
| **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 point of contact (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** |
| --- | --- |
| Review intelligence and information sharing and dissemination processes I relation to a credible threat to domestic critical infrastructure owners / operators. | * Planning * Intelligence and Information Sharing * Public Information and Warning |
| Assess information sharing capabilities with the public, sector partners, and federal, state, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures. | * Planning * Intelligence and Information Sharing * Public Information and Warning |
| Discuss private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under NIMS with local, state, and federal agencies. | * Planning * Risk Management for Protection Programs and Activities |
| [Insert objective] | * [Insert capability aligned to each objective] |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

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

* **Players:** Players have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
* **Observers:** Observers do not directly participate in the exercise. However, they may support the development of player responses to the situation during the discussion by asking relevant questions or providing subject matter expertise.
* **Facilitator:** The facilitator provides situation updates and moderates discussions. They also provide additional information or resolve questions as required. Key EPT members also may assist with facilitation as subject matter experts (SMEs) during the exercise.
* **Moderators:** Moderators are responsible for admitting and signing in all participants to the virtual exercise, monitoring the chat area for questions and / or issues, and controlling participant audio.
* **Evaluators:** Evaluators are assigned to observe and document the discussion during the exercise, participate in data analysis, and assist with drafting the After-Action Report (AAR).

## Exercise Structure

This exercise will be a discussion-based, facilitated exercise. Players will participate in the following two modules:

* Module One: Threat and Initial Incident
* Module Two: Incident and Incident Aftermath

Each module begins with a multimedia update that summarizes key events occurring within that time period. After the updates, participants review the situation and engage in discussions of appropriate [insert mission area] issues.

## Exercise Guidelines

* This exercise will be held in an open, no-fault environment wherein capabilities, plans, systems, and processes will be evaluated. Varying viewpoints, even disagreements, are expected.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing assets) and insights derived from your training.
* Decisions are not precedent setting and may not reflect your jurisdiction’s/ organization’s final position on a given issue. This exercise is an opportunity to discuss and present multiple options and possible solutions.
* Issue identification is not as valuable as suggestions and recommended actions that could improve [insert mission area] efforts. Problem-solving efforts should be the focus.
* The assumption is that the exercise scenario is plausible and events occur as they are presented. All players will receive information at the same time.

## Exercise Evaluation

Evaluation of the exercise is based on the exercise objectives and aligned core capabilities. Players will be asked to complete a participant feedback form. These documents, coupled with facilitator observations and evaluator notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

# Module One: Threat and Initial Incident

## Scenario

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

## Overseas Incident

Media outlets in the United States report that an unknown group implemented a series of cyberattacks against drinking water treatment facilities throughout [insert foreign countries]. The attacks impacted both the business and Industrial Control System (ICS) computer networks causing errors and, in some instances, the incorrect application of chemicals to the water being treated. Cities and towns within the service area of the impacted facilities issue “Do not use” orders until water can be sampled.

## Domestic Threat

A previously unknown group calling themselves “Universal Adversary” (UA) claimed full responsibility for the recent water sector attacks. They claim to be a loose collective of like-minded hackers, but do not provide a reason for the attack. A statement posted on a website known to be frequented by hackers and claiming to be from UA warns that the attack against [insert foreign countries] was a trial run in preparation for larger attacks against U.S. water sector facilities.

## Domestic Incidents

A wastewater treatment facility, [insert Name], located in [insert domestic city, state] reports to the Water Information Sharing and Analysis Center (Water-ISAC) that they discovered its ICS was accessed remotely from an IP address originating in [insert foreign country]. They are reviewing system logs to determine if any unauthorized actions were taken. A second facility, located in [insert domestic city, state] reports multiple pumping station outages. Due to the geography of the local terrain, the pumps are required to move treated water from the treatment plant to storage tanks located near the city center. Neither facility is able to confirm if the issues they are experiencing are random occurrences, or if they can be traced to the cyberattacks in Europe.

## Domestic Media Coverage

Media outlets run a detailed story on the cyber-attacks in the [insert foreign countries] and report unconfirmed rumors of attacks against several water sector facilities in the United States.

## Discussion Questions

1. What is the process by which your organization would receive intelligence and protective measure information given the threat?
   1. What organizations would you communicate with (e.g., local law enforcement agencies, your Joint Terrorism Task Force [JTTF], Federal Bureau of Investigation [FBI])?
   2. Does your organization maintain a relationship with your CISA Protective Security Advisor (PSA)? If so, do you have a rapid means of contacting them?
   3. 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 have in place?
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 are used to disseminate information?
   1. What notification capabilities (e.g., alerts, emails, telecommunications, text messages, special tools) do you use to share information and communicate protective measures for implementation?
   2. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing, such as religious customs that prohibit the use of electronic communication during specific times?
      1. If so, how will threat-based alerts and notifications be distributed to community members who follow religious customs that prohibit use of electronic communication during specific times?
5. Given current and established information sharing procedures, what types of official information are the most useful (immediate information versus analyzed information) to your organization?
   1. Does your organization perform independent analysis on information provided and, if so, describe the process?
6. In the event that your organization receive information related to potential threats against your facilities and personnel, how would you communicate this information to appropriate entities (e.g., local law enforcement agencies, JTTF, FBI, CISA PSA, etc.)?
7. If there is identified “suspicious behavior” observed at a water or wastewater facility, how do the facilities report this information locally and within the Waste and Wastewater Systems Sector?
   1. Are trends of suspicious behaviors tracked across the sector nationwide?
   2. Is your organization aware of the National Suspicious Activity Reporting (SAR) Initiative?
8. Given evidence of a credible threat to the Water and Wastewater Systems Sector, does your organization review your emergency response plans (e.g., site security plans, emergency occupancy plans, emergency action plans, or other appropriate plans)?
   1. Does your organization have policies or procedures that specifically address cyber vulnerabilities or cyber threats? What are they?
9. What protective security measures or recommendations, if any, will be employed at your organization following these international attacks?
   1. Do you coordinate protective measure implementation with any other organization within the sector, or with government entities, such as law enforcement agencies and your CISA PSA?
   2. How are the protective measures the sector has put in place communicated back to the government?
   3. How useful are the information bulletins and advisories the Department of Homeland Security (DHS) provides (e.g., a Joint Intelligence Bulletin [JIB]) that recommend protective measures?

This page is intentionally left blank.

# Module Two: Incident and Incident Aftermath

## Scenario

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

## Domestic Incident

Wastewater treatment plants and potable water treatment plants across the Unites States receive an alert from the U.S. Computer Emergency Response Team (US-CERT) after domestic intelligence agencies report increased activity on several hacker sites, including one favored by the UA.

In the early afternoon, several wastewater treatment plants report computer system outages, of which some are businesses and some are ICS, after an apparent power surge. Automated operations at water treatment facilities are placed on hold until the nature of the power outage can be determined. The Water-ISAC begins reporting that several industry partners are observing unusual activity on their networks with many ICS components offline. At a wastewater treatment plant in [insert domestic city, state], the pumps at a high capacity sewage pumping station are shut off and cannot be restarted remotely. A repair crew is dispatched to attempt a repair and implement manual override of ICS.

Water companies are forced to issue “Do not drink” and “Do not use” orders and to ask customers to limit flushing of toilets and gray water use until the outages can be resolved.

Media reports the public is growing frustrated with the water restrictions and are losing faith in the public water supply. Bottled water is selling out as soon as the shelves are restocked. In some areas with severe water restrictions, the fire department has not had sufficient water pressure to combat structure fires. While there has not been any reported loss of life, property damage has been significant as a result.

## Discussion Questions

1. What is the overall response to the water situation?
   1. What plans and procedures does your stakeholder group activate when the water situation occurs?
   2. How soon can utilities provide government agencies with an estimate of the number of customers that are affected by the large-scale disruption?
   3. How soon can utilities provide government agencies with an estimate of the extent of the potential damage to their own systems?
   4. What would be the initial response of system operators to the events described? Of the federal government?
   5. What metrics do utilities use to measure restoration progress?
   6. How are your organizations’ cyber incident response and water emergency response plans linked? Are they linked to state and local response plans?
   7. What cascading effects have you considered as part of your emergency / contingency planning? Have you shared those with the potentially affected stakeholders?
   8. What are the response priorities during this type of water incident?
2. Does your facility incident response plan contain protocols for properly responding to this and similar incidents described in the scenario update? What other protocols are included in the plan?
3. What are the key messages that need to be communicated to the public from the organization’s perspective? From a government perspective?
4. What federal, state, or local resources are available to support your response?
   1. What coordination is occurring at the federal, state, and local levels?
   2. What assets or resources are available to assist you?
   3. Do you have mutual aid or other types of agreements with federal, state, or local agencies to provide resources in an emergency? How would you request those resources?
   4. How are information and updates communicated?
5. Who are the key organizations involved in overseeing response and water restoration efforts, as well as the cyber incident?
   1. What is the overall coordination or organizational structure for the response?
   2. Who are the key private stakeholders involved?
   3. Who are the key government stakeholders involved?
   4. How do utilities set up coordination and information exchange with response agencies?
   5. How do government agencies roll up information about the incident across the region? Are there fusion centers available to facilitate information sharing?
   6. What established procedures ensure the critical information is getting to the right decision makers?
   7. How would regional coordination begin between utilities?
   8. How would regional coordination begin between jurisdictions across the region?

# 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 is 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-CI** | Homeland Security Information Network – Critical Infrastructure |
| **ICS** | Industrial Control System |
| **IP** | Improvement Plan |
| **ISAC** | Information Sharing and Analysis Center |
| **JIB** | Joint Intelligence Bulletin |
| **JTTF** | Joint Terrorism Task Force |
| **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 |
| **UA** | Universal Adversary |
| **US-CERT** | United States – Computer Emergency Response Team |

