Electric Substation Sabotage Tabletop Exercise

Situation Manual

[Insert Date]

**\*[Insert Caveat]\***

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

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 7:45 a.m. | 8:30 a.m. | Registration |
| 8:30 a.m. | 8:45 a.m. | Welcome and Participant Briefing |
| 8:45 a.m. | 10:15 a.m. | Module One: Incident Detection, Notification, and Reporting |
| 10:15 a.m. | 10:30 a.m. | Break |
| 10:30 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** | Electric Substation 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 [insert other Mission Areas] |
| **Capabilities** | Planning, Intelligence and Information Sharing, Risk Management for Protection Programs and Activities, and Public Information and Warning. |
| **Objectives** | 1. Identification of key regional and local critical infrastructure stakeholders and facilities. 2. Review of incident reporting, intelligence threat warning, and information sharing and dissemination processes between state, local, tribal, and territorial entities; law enforcement; facility owners and operators; and federal departments and agencies in relation to a credible threat to, a security incident at, or attack on, regional or local critical infrastructure. 3. Discuss regional and local stakeholders’ emergency preparedness plans and procedures to a security incident or attack on an electric substation and the coordination of activities under the National Incident Management System (NIMS) with federal, state, local, tribal, and territorial entities.   [Insert additional exercise objectives as necessary] |
| **Threat or Hazard** | Sabotage Incident |
| **Scenario** | An attack targeting equipment disrupts an electric power grid at an electric substation. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, 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).] |

This page is intentionally left blank.

# General Information

## Exercise Objectives and Capabilities

The exercise objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to capabilities, which are the means to accomplish a mission, function, or objective based on the performance of related tasks, under specified conditions, to target levels of performance. The objectives and aligned capabilities are guided by senior leaders and selected by the Exercise Planning Team (EPT).

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Identification of key regional and local critical infrastructure stakeholders and facilities. | * Planning |
| Review of incident reporting, intelligence threat warning, and information sharing and dissemination processes between state, local, tribal, and territorial entities; law enforcement; facility owners and operators; and federal departments and agencies in relation to a credible threat to, a security incident at, or attack on, regional or local critical infrastructure. | * Public Information and Warning * Intelligence and Information Sharing |
| Discuss regional and local stakeholders’ emergency preparedness plans and response procedures to a security incident or attack on an electric substation and the coordination of activities under National Incident Management System (NIMS) with federal, state, local, tribal, and territorial entities. | * Risk Management for Protection Programs and Activities * Public Information and Warning |
| [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:** 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.
* **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: Incident Detection, Notification, and Reporting
* 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 notes, will be used to evaluate the exercise and then compiled into the AAR / Improvement Plan (IP).

# Module One: Incident Detection, Notification, and Reporting

## Scenario

## [Insert Location]

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

In [Insert location], local police receive multiple reports of individuals taking photographs of transmission lines, transformers, and electric substations. Although no suspects were questioned to date, some reports indicate that the individual may have been dressed in a uniform resembling those local utility workers wear and may have had a backpack containing tools. Concurrently, [Insert electric company] observed some suspicious activity at a few of its electric substations.

Recently, the Federal Bureau of Investigation (FBI) released a Joint Intelligence Bulletin (JIB) warning of possible sabotage to telephone lines, specifically those relating to 911 services. In response to the JIB, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) issued an industry advisory concerning the need for increased vigilance and reporting of suspicious activity.

## Discussion Questions

1. Has the industry identified to law enforcement the level of importance of regional and local critical infrastructure (e.g., electric substation, communications, and electrical vaults)?
2. What security or intruder detection measures are employed at both above ground and underground communication vaults?
3. What security or intruder detection measures are employed at local electric substations?
4. If your organization received information related to “suspicious behavior” or potential threats against your facilities and personnel, how would you communicate this information to appropriate industry partners, law enforcement, and homeland security entities?
   1. What are your local reporting procedures (e.g., local suspicious activity reporting [SAR]), and which entities would you notify?
   2. Is your organization aware of the Nationwide SAR Initiative?
   3. How would you report the information within the Electricity Subsector?
   4. Does your organization participate in cross-sector information sharing or threat warning coordination?
   5. Is your organization familiar with how to contact your local law enforcement, Joint Terrorism Task Force (JTTF), state fusion center, and FBI Office?
   6. Does your organization maintain a relationship with your CISA Protective Security Advisor (PSA)?
   7. Does your organization maintain a relationship with state or federal security or regulatory-related entities (e.g., CISA Chemical Facility Anti-Terrorism Standards Chemical Inspectors, U.S. Coast Guard, U.S. Department of Transportation, Environmental Protection Agency)?
5. What measures might you ask of local law enforcement at this time to protect your organization and / or facilities (e.g., outreach, increased vigilance)?
6. What internal information sharing and dissemination processes does your organization currently use?
   1. How does your organization triage the information it receives (e.g., formal reporting, rumors, social media) for further dissemination within the organization and to personnel?
   2. Are nationwide trends of suspicious behaviors within your industry and across the Energy Sector tracked locally?
   3. Who is responsible for coordinating the risk communications message for your organization?
   4. How would implementation of protective measures be communicated (e.g., alerts, emails, telecommunications, text messages, special tools)?
   5. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing or prohibit use of electronic communication during specific times?
7. 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 use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?
   2. Does your office habitually receive ES-ISAC Industry Advisories or JIBs that are pertinent to your organization?
   3. Does your organization receive security threat or protective measure information from trade organizations, manufacturers, consultants, or other industry partners?
   4. Does your organization perform independent analysis on information provided? If so, describe the process?

# Module Two: Incident and Incident Aftermath

## Scenario

## [Insert Location]

### [Insert Month, Day, Year]: 12:46 AM

Residents within [insert location] experience disruptions in attempts to place and receive 911 calls using their landline telephones. Citizens that were unable to place landline calls successfully used mobile telecommunications to notify 911 operators and their telephone service providers of the problem.

The location of the communications disruption is determined to be near the [insert specific substation], located outside of [insert location]. [Insert telecommunication company] workers are dispatched to the site and begin surveying to determine the locality and cause of the disruption.

### [Insert Month, Day, Year]: 1:48 AM

Law enforcement officers are dispatched to [insert specific substation] electric substation after receiving reports of sporadic gunfire being directed at the substation. Meanwhile, [insert electric utility company] facility operators notice system abnormalities and begin implementing safety protocols. After a cursory search around the perimeter of the substation facility, police officers discover several “large metal boxes” leaking fluid, possibly oil.

Upon analysis, the local fusion center determines that this closely resembles an event outlined in an ES-ISAC Industry Advisory dated [insert date]. When this information is forwarded to the local FBI Field Office, they issue a JIB for release to local law enforcement and the private sector, stating that this is a recurring method of sabotage.

## Discussion Questions

1. Would the electric utility company be notified by the telecommunications company of the communications disruption or vice versa of any power disruption?
   1. Would the 911 dispatch office contact either the electric company or telecommunication company to report any disruption of service or inquire about the duration for repair?
   2. Should there be more sharing of real-time information between telecommunication and electric substation entities, particularly when interruption of communications may be an initial sign of an attack?
2. Are first responders (e.g., law enforcement, fire fighters, and emergency services) aware of any specific concerns or hazards associated with responding to incidents at electric substations?
3. Do your organization’s emergency response plans (e.g., site security plans, emergency evacuation plans, emergency action plans, or other appropriate plans) contain protocol for properly responding to incidents described in this module?
   1. How often does your organization review its emergency response plans, and does it perform drills to test their effectiveness?
   2. Do your organization’s response plans address how to coordinate power restoration priorities?
   3. Do your organization’s response plans account for law enforcement evidence-gathering requirements?
   4. Have cross-sector dependencies been incorporated into your organization’s response plans?
   5. Have resulting impacts or cascading effects on other electricity components within the Energy Sector been incorporated into your organization’s response plans?
4. What information sharing processes would you use to disseminate information concerning this incident?
   1. What notification capabilities (e.g., alerts, emails, telecommunications, text messages, special tools, or HSIN) would you use to share information and communicate protective measures implementation?
   2. How would employee safety concerns be managed (e.g., at what point would the utility company allow employees to enter the site)?
   3. What are your organization’s external information sharing responsibilities in response to this incident?
   4. How would proprietary information concerns be managed?
   5. Are there technological barriers, legal considerations, or institutional sensitivities that might affect information sharing or prohibit use of electronic communication during specific times?
5. What protective security measures would be employed following a domestic attack?
   1. Would you coordinate protective measure implementation with any organization within the Electricity Subsector or specific government entities, such as law enforcement agencies and your CISA PSA?
   2. Would you need to communicate implemented protective measures to organizational liaisons, response entities (e.g., Joint Field Office Unified Command), or other industry or government partners (e.g., Public Utility Commissioner)?
   3. How useful are the information bulletins and advisories the U.S. Department of Homeland Security (DHS) provides (e.g., a JIB) that recommend protective measures?
6. What measures would local law enforcement take at this time to protect your organization (e.g., outreach, increased vigilance)?
7. How would you coordinate public messaging concerning the continuing credible threat to your organization and stakeholders?
   1. What organizations would you coordinate this messaging with?

# 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 |
| **ES-ISAC** | Electricity Sector Information Sharing and Analysis Center |
| **FBI** | Federal Bureau of Investigation |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **IP** | Improvement Plan |
| **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 |

