[Insert Picture of Your Facility]

Chemical Sector Theft & Diversion Tabletop Exercise

Situation Manual

[Insert Date]

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

This Situation Manual (SitMan) provides exercise participants with all 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. | 9:45 a.m. | Module One: Pre-Incident |
| 9:45 a.m. | 9:55 a.m. | Break |
| 9:55 a.m. | 10:55 a.m. | Module Two: Incident |
| 10:55 a.m. | 11:05 a.m. | Break |
| 11:05 a.m. | 11:30 a.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Chemical Sector Theft & Diversion 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** | * Economic Recovery * On-Scene Security, Protection, and Law Enforcement * Operational Communications * Operational Coordination * Planning * Public Information and Warning * [insert other capabilities] |
| **Objectives** | 1. Review emergency preparedness plans and response procedures for a theft and diversion incident at a chemical sector owner’s / operator’s facility. 2. Discuss the coordination between private sector organizations and responding local, state, and federal agencies under the National Incident Management System (NIMS). 3. Assess procedures for coordinating and sharing information within organizations, between organizations, and with the public. 4. Review organizational interdependencies. 5. [Insert additional exercise objectives as necessary] |
| **Threat or Hazard** | Theft / Diversion |
| **Scenario** | An interactive, discussion-based exercise focused on an attempted theft at a chemical sector facility. The scenario consists of two modules: Pre-Incident and Incident |
| **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 Point of Contact (POC) (e.g., exercise director or exercise sponsor).] |

# 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).

For additional information regarding core capabilities, please visit:

<https://www.fema.gov/emergency-managers/national-preparedness/mission-core-capabilities>

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Review emergency preparedness plans and response procedures for a theft and diversion incident at a chemical sector owner’s / operator’s facility. | * On-Scene Security, Protection, and Law Enforcement * Operational Communication * Operational Coordination * Planning |
| Discuss the coordination between private sector organizations and responding local, state, and federal agencies under NIMS. | * Operational Communication * Operational Coordination * Planning |
| Assess procedures for coordinating and sharing information within organizations, between organizations, and with the public. | * Operational Communication * Operational Coordination * Planning |
| Review organizational interdependences. | * Economic Recovery * Operational Coordination * Planning |
| [Insert additional objectives as necessary] | * [Insert additional capability 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** are 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.
* **Facilitators** provide 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.
* **Data Collectors** 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: Pre-Incident
* Module Two: Incident

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] issues. 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: Pre-Incident

## Scenario

## [Insert Location]

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

It is a busy morning at [insert name of facility], and employees are steadily beginning their morning routines. Several employees go to check on equipment while others walk around the facility. As they’re walking around the facility, two employees notice a grey van with tinted windows they do not recognize parked outside of the facility grounds. Not thinking much of it, the employees continue their walk toward their workstations.

Later in the day, a [insert name of facility] security officer making his rounds on the property notices a portion of fence bordering the facility has been cut. The officer files an internal report detailing his observations, and maintenance is scheduled to repair the fence.

## Discussion Questions

1. Does your facility have security cameras that are routinely checked?
   1. If not, what is the protocol for checking for security breaches?
2. Does your facility have a threat management or threat assessment team to address suspicious or potentially threatening behavior?
3. How are your employees trained on identifying security threats?
   1. Is the training completed during onboarding or done regularly throughout the year?
   2. Are training materials easily accessible or posted where employees have them readily available?
   3. Does the training teach employees how to document and report suspicious activity?
   4. Do employees know who to contact with questions or concerns related to suspicious activity?
4. Has your facility previously needed to contact law enforcement for a similar situation?
   1. What are your written procedures for involving law enforcement in a possible suspicious activity incident?
5. Is your company familiar with federal resources available for consultation once a threat management team opens a case, such as the U.S. Secret Service (USSS) National Threat Assessment Center?

a. What organizations would you communicate with regarding the incident (e.g., local law enforcement, joint terrorism task force (JTTF), fusion centers, etc.)?

b. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?

This page is intentionally left blank.

# Module Two: Incident

## Scenario

## [Insert Location]

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

## Option A: Nefarious Chemical Mislabeling

The next morning, employees are arriving to work at [insert chemical facility name]. As personnel working in the chemical labeling department begin taking inventory of the chemicals they oversee, one employee notices several 1-gallon containers of [insert chemical type] have been re-labeled as hydrogen peroxide. Upon further observation, the employee realizes the same number of hydrogen peroxide containers are missing from the chemical storage area.

Due to an uptick in recent security reports, the employee quickly alerts his manager to the missing materials. As word of the incident travels around your facility, another employee recalls that an unknown vehicle had been parked in front of the facility the day before and reports the grey van sighting to their manager. Security employees work to acquire surveillance tapes from inside and outside the facility to identify possible suspects in the missing materials.

After reviewing the tapes and being unable to identify two suspicious persons, security personnel file a report with the local police department. Employees detail their observation of the grey van, the report of the vandalized fence, and provide identification information for the stolen chemicals. Law enforcement launches an investigation.

## Scenario

## [Insert Location]

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

## Option B: Accidental Operational Miscalculation

The next day as employees are arriving to work at [insert chemical facility name], personnel notice a discrepancy in the amount of [insert chemical name] used for [insert process relevant to the facility].

Although [insert relevant amount of chemical] is typically used for [insert name of process], the current chemical volume in [insert type of container chemical would be stored in] reads as [insert lower amount relative to original amount] – lower than it should be, given the facility’s recent usage needs.

In the wake of the vandalized fence and suspicious van parked outside of the facility the day prior, personnel begin an investigation into possible suspects who may have been inside the facility before the chemical reports were made.

Upon reviewing records from the day before, the employees realize that an inventory cycle count had been completed by a new employee and had been inaccurately represented in the prior day’s reports. The investigation into possible suspects is halted.

## Discussion Questions

1. What plans exist to prevent or deter a theft at your facility?
   1. Who is responsible for the security plan and necessary updates?
   2. Are multiple agencies outside of your organization involved in the response and recovery planning process?
   3. What security measures exist to detect and delay an adversary from perpetrating a vehicle theft (i.e., identification checks, traffic control, key control program, global positioning system [GPS] / vehicle locators, etc.)?
      1. What are your facility’s procedures for shipping, receiving, and storing hazardous chemicals?
   4. What type of inventory management system exists at the facility?
      1. What type of procedures exist to report and respond to lost and stolen chemicals?
2. How are security and personnel trained regarding theft?
   1. What training programs exist for personnel? Who trains them?
   2. How are personnel trained to respond to a chemical theft?
   3. What are the rules of engagement for your security personnel?
   4. What is the chain of command for on-site security personnel?
   5. Have security personnel had the opportunity to coordinate with local law enforcement?
   6. Which organizations contribute to your facility’s security?
3. Do your organization’s standard operating procedures (SOPs) for incident response include roles and responsibilities for staff?
   1. Do your organization’s SOPs include roles and responsibilities for scene security and evidence preservation?
4. What assets are on-site to immediately respond to an incident?
   1. What resources are available that would help with response?
5. What resources does your organization use to disseminate information?
   1. What notification capabilities (e.g., alerts, emails, telecom, text messages, etc.) does your organization use to share information and communicate incidents?
   2. Who is responsible for sending out the alerts or warnings?
   3. What protocols exist for alerting employees to an incident?
      1. Does your organization have pre-built public information templates for use in different kinds of emergencies?
   4. Do you have established protocols for alerting other businesses to thieves in the area?
6. Given the scenario, does your emergency action plan (EAP) include measures for protecting the security of chemicals at your facility?
7. Who is responsible for ensuring chemical security measures are met?
8. How often are personnel trained?
   1. Is training part of onboarding only, or is it recurring?
9. How does the human resources department communicate with management in the event of terminations / employee counseling?
   1. What are procedures for turning in access cards / keys?
10. How does your company’s security posture differ between working hours and non-working hours?
11. What physical security measures exist to detect and delay an adversary from getting on-site?
    1. What are your delay measures (e.g., fences, barriers, access controls systems, etc.)?
    2. What are your detection measures (e.g., intrusion detection systems, closed-circuit television [CCTV], facility personnel / on-site security, etc.)?
    3. Are these physical security systems tested and inspected for effectiveness?
12. What plans exist to prevent or deter an attack of this type at your facility?
    1. What threats are you most concerned with preventing?
    2. Who is responsible for the security plan and necessary updates?
    3. Are multiple agencies outside of your organization involved in the response and recovery planning process?
    4. What plans exist to deter / prevent an intrusion at your facility (e.g., screening, security presence, etc.)?
13. In the event of a credible threat to the Chemical Sector, what specific actions and / or protective measures would your company / facility take in response to the threat information? What avenues are available to your facility to request more details regarding this threat?
    1. If your facility is covered by regulations (e.g., Chemical Facility Anti-Terrorism Standards [CFATS], Maritime Transportation Security Act [MTSA], etc.), has it complied with required standards?
       1. What documents guide your company / facility in a credible threat environment?
       2. Are the documents readily available to everyone with a need-to-know?
       3. Would your facility activate specific planning or operational capabilities, including business continuity plans?
       4. Would your facility share these specific measures with local, state, and federal partners?
       5. Who makes the decision to activate specific planning or operational capabilities, and how quickly is the decision made?
14. What are your organization’s information sharing responsibilities at this point in an incident?
    1. What formal information sharing processes would your organization use at this point?
    2. What resources are used to disseminate information?
    3. Who would be responsible for public messaging in your organization (if applicable)?
       1. Would your messaging be coordinated with any other organizations? If so, how?
    4. How would you send information to your employees?
    5. How would you send information to your patrons or customers (if applicable)?
    6. Who is responsible for communicating information to potentially impacted businesses?
    7. What are your communication goals?
15. Who is responsible for notifying state or federal agencies to the incident, and at what point in the incident would this occur?
    1. What resources or actions would you expect from state or federal agencies?
    2. How would arriving state and federal resources integrate into the command structure, if at all? At which locations (Unified Command, Area Command, emergency operations center [EOC], multi-agency coordination [MAC] Group, etc.)?
    3. Do you share information with your state fusion center?
16. What role do city and county governments play in this scenario?
    1. Who is responsible for informing the mayor, county commissioners, or other local elected officials?
    2. Have protocols been established with elected officials so that they know what to expect during incident response? Do local agencies know what elected officials’ priorities are?
    3. Is there a location (such as an EOC) where elected officials will know to go to during an incident?
       1. If so, where is it?
17. Does your facility or organization have a designated public information officer (PIO)? If so:
    1. Do protocols exist for addressing media inquiries?
    2. How does the media receive information from the incident?
    3. Does the PIO have pre-built public information templates for use in different kinds of emergencies?
    4. Would your organization use social media during an incident?
18. Following this incident, what additional protective measures will be put into place at your organization?
    1. How would information on protective measures be obtained?
    2. How would any relevant classified information be shared, and do you have staff on board with security clearances?
    3. How is relevant information shared within your critical infrastructure sector?
       1. How do you communicate information to other members of your sector or receive information from them?
       2. Do you know how to contact your Sector-Specific Agency (SSA)?
       3. Do you have a Homeland Security Information Network (HSIN) account?
    4. Do you know how to contact your CISA Protective Security Advisor (PSA)?
19. How would your organization manage the fallout from the incident?
    1. How would you manage the potential cascading effects of this incident down the line?

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 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 |
| **CCTV** | Closed-Circuit Television |
| **CFATS** | Chemical Facility Anti-Terrorism Standards |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **EAP** | Emergency Action Plan |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **GPS** | Global Positioning System |
| **HSIN** | Homeland Security Information Network |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **IP** | Improvement Plan |
| **JTTF** | Joint Terrorism Task Force |
| **MAC** | Multi-Agency Coordination |
| **MTSA** | Maritime Transportation Security Act |
| **NIMS** | National Incident Management System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **SSA** | Sector-Specific Agency |
| **TTX** | Tabletop Exercise |
| **USSS** | United States Secret Service |

This page is intentionally left blank.

