[Insert Picture of Your Facility]

Chemical Sector Insider Threat 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. | 10:00 a.m. | Break |
| 10:00 a.m. | 11:00 a.m. | Module Two: Incident |
| 11:00 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 Insider 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** | * Intelligence and Information Sharing
* On-scene Security, Protection, and Law Enforcement
* Operational Communications
* Operational Coordination
* Planning
* Situational Assessment
* [Insert other capabilities]
 |
| **Objectives** | 1. Examine organizational recovery procedures and recovery operations coordination across stakeholder groups.
2. Review intelligence and information sharing processes, and examine plans for addressing a potential insider threat.
3. Discuss private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident and coordination activities under the National Incident Management System (NIMS) with local, state, and federal agencies.
4. Assess the existing methods and effectiveness of internal and external communications and coordination during and / or immediately after becoming aware of an adversarial event.
5. Discuss gaps and challenges in private sector stakeholders’ emergency preparedness plans and response procedures to a cyber-related incident.
6. [Insert additional exercise objectives as necessary]
 |
| **Threat or Hazard** | Insider Threat |
| **Scenario** | An interactive, discussion-based exercise focused on an insider threat 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** |
| --- | --- |
| Examine organizational recovery procedures and recovery operations coordination across stakeholder groups. | * Operational Communication
* Operational Coordination
* Planning
* Situational Assessment
 |
| Review intelligence and information sharing processes and examine plans for addressing a potential insider threat. | * Intelligence and Information Sharing
* On-scene Security, Protection, and Law Enforcement
* Operational Communication
* Planning
* Situational Assessment
 |
| 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. | * Intelligence and Information Sharing
* On-scene Security, Protection, and Law Enforcement
* Operational Communication
* Operational Coordination
* Planning
 |
| Assess the existing methods and effectiveness of internal and external communications and coordination during and / or immediately after becoming aware of an adversarial event. | * Intelligence and Information Sharing
* Operational Communication
* Operational Coordination
* Planning
* Situational Assessment
 |
| Discuss gaps and challenges in private sector stakeholders’ emergency preparedness plans and response procedures to a cyber-related incident.  | * Intelligence and Information Sharing
* Operational Coordination
* Planning
 |
| [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** 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.
* **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.
* **Date 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]

Over the last couple of weeks, [insert organization] received an increased number of complaints about an employee that many describe as “disgruntled.” According to the complaints, John Doe has been talking to his coworkers about his distaste with the way management is handling his pay. A few coworkers are aware of a rumor that has spread about his pending divorce, which they believe aggravated his temperament at work.

On a quiet morning in the office, one of John Doe’s coworkers hears him yelling at someone over the phone in the men’s break room. He is explaining that his supervisor is unwilling to give him a raise after several months of working for [insert organization].

Upon hearing of the break room phone conversation, John Doe’s supervisor requires he come to the office where they discuss the ongoing issues with his behavior at work. The supervisor also addresses ongoing issues with John Doe’s poor performance and informs him that he will be placed on a probationary period. The supervisor warns him that if his work and behavior do not improve, there will be steeper consequences.

John Doe exclaims he does not wish to discuss anything further, abruptly exits the office and slams the door, garnering the attention of nearby employees.

## Discussion Questions

1. What training on dealing with insider threats is available to employees?
	1. Is the training mandatory for all employees?
		1. Does preliminary training occur during onboarding?
		2. Does this include refresher trainings annually or throughout employment?
		3. Is there a distinction between the material offered during onboarding versus that which is provided later during employment?
	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 behavior?
	4. Does the training include information and protocols for addressing cyber threats from insiders?
	5. Do employees know who to contact with questions and concerns relating to insider threats?
	6. Does this training address potentially dangerous chemicals employees should be aware of that a disgruntled employee could use maliciously?
2. Should employees who witness their coworkers engage others as described in this incident, whether over the phone or in person, take any action?
	1. Are there plans or procedures available to guide employees in their actions / decisions?
	2. Is there a way for employees to report non-violent suspicious behavior?
	3. Do you have a threat assessment / crisis intervention team on-site who can attempt to de-escalate the employee?
3. Has your facility previously needed to contact law enforcement for a similar scenario?
	1. What are your written procedures for involving law enforcement in a possible insider threat and theft incident?
4. Is your company familiar with federal resources available for consultation once a threat management team[[1]](#footnote-1) opens a case, such as the U.S. Secret Service (USSS) National Threat Assessment Center?
	1. What organizations would you communicate with regarding this incident (e.g., local law enforcement, Joint Terrorism Task Force [JTTF], fusion centers, etc.)?
	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?
		1. What is your facility’s policy on contacting your PSA versus contacting law enforcement? Who would be contacted first in an incident such as this one?
	3. Does your organization use the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) portal?
5. What actions, if any, should the supervisor take after meeting with the employee?
	1. What actions could have been taken to reduce disruptive behaviors?
		1. Should the employee’s behavior be reported to security? Should he have been escorted out, and if so, by whom?
		2. If an employee were to be terminated, what protocols, if any, are in place to rescind access to company property and information systems?
	2. Did any of the supervisor’s actions potentially increase insider threat risk factors?
6. Are there counseling services available to employees who show signs of stress or aggression?
7. Are facility / company policies adequate to de-escalate this from evolving into an incident? Are there any ways policies could be improved?
	1. Are there existing policies to prevent the disgruntled employees from removing and using dangerous chemicals?
8. Does your company use background checks or any screening practices when selecting new employees?

This page is intentionally left blank.

# Module Two: Incident

## Scenario

## [Insert Location]

### [Insert Month, Day, Year + 5 Days]

## Option 1: Short-Term, High Volume Theft

It is a busy morning at [insert facility], and several days have passed since the meeting between John Doe and his supervisor. There have been no further incidents from John Doe after the disciplinary action taken, and he reports to work to begin his shift.

Later that day, as several employees break for lunch, John Doe logs into the [insert facility]’s inventory control system with his own personal password and credentials. He manipulates the system to route a five-gallon portion of a recently received shipment of aluminum powder, a chemical that is known to be used as a precursor in homemade explosives, from the facility to his personal home address. He then falsifies the records database within the inventory control system so that it shows that [insert facility] still has the full shipment of aluminum powder on-site.

John Doe logs out of the inventory control system just before his coworkers return from lunch and report back to their respective workstations. [Insert facility] carries on normally throughout the rest of the day with no one aware of the inventory manipulation.

John Doe’s behavior continues to escalate resulting in further disciplinary action and, finally, his eventual termination two weeks post-theft of the aluminum powder. There are rumors circulating that he may have stolen product from the facility, and [insert facility] launches an investigation.

## Scenario

## [Insert Location]

### [Insert Month, Day, Year + 6 Months]

## Option 2: Long-Term, Low Volume Theft

Over the last several months, [insert facility] had tasked Jane Smith with ordering and receiving aluminum powder shipments and John Doe with checking and extracting the powder for processing.

Six months after John Doe spoke with his supervisor, an internal company audit of the [insert facility]’s inventory shows a discrepancy in the number of aluminum pails logged in the inventory control system.

Outbound shipping logs show several unauthorized shipments of one-pound portions of powder to a nearby residential address. The shipments left the facility on various dates during the prior six months.

Upon researching employee records, it is discovered that the residential address matches the address where John Doe lives. [Insert facility] contacts the local police department, chemical security inspectors, and its CISA PSA to report the missing aluminum powder incident; an investigation is launched.

## Discussion Questions

1. What preventative physical security and cybersecurity measures regarding access to inventory control systems are in place at your facility?
2. Does your facility carry out physical inventory checks on explosive pre-cursor materials where small amounts could be taken over a long period of time without detection?
	1. How often are formal inventories completed on chemicals of interest or hazardous materials?
	2. Describe the facility’s response procedures when a product is determined to be lost. If this is a Chemical Facility Anti-Terrorism Standards (CFATS) covered facility, has the assigned Chemical Security Inspector (CSI) been notified and a report filed?
3. What verification methods exist with respect to the processing and receiving of chemical shipments, particularly potentially hazardous materials?
4. What restrictions are placed on or considerations given to employees who have received disciplinary action?
5. What are your organization’s information sharing responsibilities in response to the incident?
6. What formal information sharing processes would your organization use at this point?
7. What resources are used to disseminate information?
	1. What notification capabilities (e.g., alerts, emails, telecommunications, text messages, special tools) does your organization employ to share information and communicate protective measures implementation?
	2. Are there technological barriers, legal considerations, or institutional sensitivities that might affect or limit information sharing, such as religious customs that prohibit use of electronic communications during specific times?
		1. If so, how will threat-based alerts be distributed to community members who might not receive the latest alert through electronic communication methods?
8. What measures would local law enforcement take at this time to protect your organization (e.g., improved cybersecurity, employee training, increased vigilance, etc.)?
9. How do the facility’s incident response plans address the events described in this module?
	1. Is there security on-site at your facility?
		1. How does your company protect precursor materials from being compromised or stolen? Does it have a least privilege policy to limit the number of employees with access?
10. What specific actions and / or protective measures would your company / facility take in response to the incident?
	1. If your facility is covered by regulations (CFATS, etc.), has it complied with required standards?
	2. What documents guide your company / facility in a credible threat environment?
	3. Is the document readily available to everyone with a need-to-know?
	4. Would your facility activate specific plans, including business continuity plans?
	5. Would your facility share these specific measures with local, state, and federal partners?
	6. Who makes the decision to activate specific planning or operational capabilities, and how quickly is the decision made?
11. Is there an established business continuity, continuity of operations (COOP), or rapid recovery plan that addresses this type of incident?
	1. How will the facility address any impediments to operations?
	2. Are there any potential liability issues from this incident that facility managers would be addressing at this point?
12. What protective security measures will be employed at your organization following this incident?
13. What information sharing mechanisms are in place that could be relevant for an incident such as this?
	1. What information on the incident would owners / operators share with other employees, and how would this be done?
	2. What information about this attack would owners / operators share with other facilities in their company or sector?
	3. What mechanisms would owners / operators use to relay information to federal, state, or local authorities?
	4. Do you share information with your local / state fusion center?
14. How would owners / operators expect to receive information from their federal, state, and local officials?
15. How can owners / operators prepare to handle the public messaging / media in the aftermath of such an occurrence?
16. Following this incident, what additional protective measures would your organization put into place, if any?
	1. How would your organization obtain information on protective measures?
	2. How would your organization share any relevant classified information?
	3. Do any of your employees hold security clearances?
	4. How does your organization share relevant information within your critical infrastructure sector?
		1. How does your organization 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)?
	5. Do you know how to contact your CISA PSA?
	6. If you are a CFATS covered facility, do you know how to contact your CISA CSI?

### *Cyber-Specific Activities*

1. What types of cybersecurity policies, plans, and / or protocols does your company have to detect, respond to, and recover from a cyberattack?
2. Who would your organization contact internally or externally about the cyber element of the incident?
3. What internal and external messages should be developed regarding the cyber element of the incident? How are they distributed?
4. What protocols exist in your facility to address such an event?
	1. Are there cyber detection, prioritization, and response capabilities within your organization’s protocols?
	2. Do employees know what constitutes suspicious cybersecurity activities or incidents?
	3. Do employees know what actions to take when one arises?
5. Would this incident trigger contact with regulators?
	1. If so, when would your organization make contact?
6. If chemical inventory systems are compromised, do you have backup manual procedures for these systems?
7. If inventory control systems are compromised, what cascading impacts may occur both internally to your facility and externally to other stakeholders / community members?
8. Given the scenario, does your emergency action plan (EAP) include measures for protecting the security of chemicals at your facility?
9. Who is responsible for ensuring chemical security measures are met in your facility?

# 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 |
| **CFATS** | Chemical Facility Anti-Terrorism Standards |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **COOP** | Continuity of Operations |
| **CSI** | Chemical Security Inspector |
| **CTEP** | CISA Tabletop Exercise Package |
| **EAP** | Emergency Action Plan |
| **EPT** | Exercise Planning Team |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **IP** | Improvement Plan |
| **JTTF** | Joint Terrorism Task Force |
| **NIMS** | National Incident Management System |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert |
| **SSA** | Sector-Specific Agency |
| **TTX** | Tabletop Exercise  |
| **USSS** | United States Secret Service |

This page is intentionally left blank.



1. U.S. Department of Homeland Security, *Threat Assessment and Management Teams*, (U.S. Department of Homeland Security, 2021), <https://www.dhs.gov/publication/threat-assessment-and-management-teams> [↑](#footnote-ref-1)