[Insert Cover Picture]

Chemical Sector Fire as a Weapon 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 |
| --- | --- | --- |
| 12:30 p.m. | 1:00 p.m. | Welcome and Introductions |
| 1:00 p.m. | 1:45 p.m. | Module One: Threat |
| 1:45 p.m. | 2:00 p.m. | Break |
| 2:00 p.m. | 2:45 p.m. | Module Two: Incident |
| 2:45 p.m. | 3:00 p.m. | Break |
| 3:00 p.m. | 3:45 p.m. | Module Three: Recovery |
| 3:45 p.m. | 4:00 p.m. | Hot Wash / Closing Remarks |

*\* All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Chemical Sector Fire as a Weapon 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** | * Facility Management Services
* Intelligence and Information Sharing
* Operational Coordination
* Planning, Public Health and Medical Services
* Public Information and Warning
* Situational Assessment
 |
| **Objectives** | 1. Examine pre-incident and incident intelligence and information sharing procedures between public and private sector stakeholders.
2. Examine emergency response plans and procedures during a complex coordinated attack with a focus on Incident Command System / National Incident Management System, Evacuation Procedures, and Public Messaging Protocols.
3. Examine recovery plans following an attack.
4. [Insert additional exercise objectives as necessary]
 |
| **Threat or Hazard** | Threat from an employee in the workplace who uses fire as a weapon. |
| **Scenario** | A disgruntled employee starting a fire in the workplace. |
| **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).] |

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** |
| --- | --- |
| Examine pre-incident and incident intelligence and information sharing procedures between public and private stakeholders. | * Intelligence and Information Sharing
* Planning
 |
| Examine emergency response plans and procedures during a complex coordinated attack with a focus on:* Incident Command System / National Incident Management System
* Evacuation Procedures
* Public Messaging Protocols
 | * Facility Management Services
* Intelligence and Information Sharing
* Operational Coordination
* Planning
* Situational Assessment
 |
| Examine recovery plans following an attack. | * Health and Social Services
* Operational Coordination
* Planning
* Public Health and Medical Services
* 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:** 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 three modules:

* Module One: Threat
* Module Two: Incident
* Module Three: Recovery

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).

This page is intentionally left blank.

# Module One: Threat

## Scenario

## [Insert Location]

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

Over the last couple of weeks, [insert organization] receives an increased number of complaints about an employee, John Doe, who many claim to be disgruntled. [Insert name]’s supervisor confirmed issues related to absenteeism, mediocre performance, and poor attitude in the past, but more recent complaints have to do with [insert name]’s temperament and verbal altercations with co-workers. According to the recent complaints, [insert name] has been demonstrating aggressive behavior because he disagrees with current regulations and company health and strategy policies. A few co-workers are aware of a circulating rumor about his pending child custody battle with his ex-wife. They believe this is triggering his behavior at work.

On a busy morning, the Human Resources department receives an email from another employee about disturbing messages [insert name] has posted on social media. Initially, the posts had to do with [insert name]’s belief that company policy is interfering with the ability to conduct business, but soon escalated to include beliefs that the company is controlling employees and violating their human rights. The most recent posts then became aggressive when [insert name] began discussing rebellion, non-compliance, and even using violence to “fight the system” on his social media accounts. Co-workers become drastically frightened and flood the Human Resources department with complaints when [insert name] posts about vulnerabilities with specific references to the facility and certain departments within.

With the abundant number of complaints and proof of his social media posts, [insert name]’s supervisor calls for an immediate meeting to sit down with [insert name] to get some clarity about the situation, and discuss his current performance and behavior to potentially mitigate any issues. The meeting does not go as planned, and once confronted, [insert name] becomes aggressive and verbally abusive, just as he had previously been with his co-workers. The meeting concludes with [insert name] making a direct threat against his supervisor and facility. [Insert name] then storms out of the office just as the supervisor attempts to call for security. Before the supervisor can complete the call, [insert name] leaves and can be seen speeding out of the parking lot.

## Discussion Questions

1. What training regarding insider threats and workplace violence is available to employees at your facility?
	1. Is the training mandatory?
	2. Does the training instruct employees how to document and report suspicious behavior?
	3. Does the training include information and protocols for addressing workplace violence?
	4. Does the training include information and protocols for addressing destructive behavior, such as theft, vandalism, and sabotage?
	5. Does the training include information and protocols for addressing cyber threats from insiders?
	6. Do employees know who to contact with questions and concerns relating to insider threats?
2. Should co-workers who witnessed this incident take any action?
	1. Are plans or procedures available at your facility to guide employees in their actions / decisions?
	2. Is there a system in place for employees at your facility to report signs of potentially aggressive / violent behavior in the workplace?
	3. Is there a way for employees at your facility to report non-violent suspicious behavior?
3. Does your facility have a threat management or threat assessment team to address suspicious or potentially threatening behavior?
4. Does your facility have policies or protocols in place to deal with employees that exhibit signs of stress, aggressive behavior, or pose a threat to the facility and its employees?
	1. Would those policies / protocols include notifying law enforcement?
5. What capabilities does your facility have to monitor potential social media threats from employees?
6. 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?
	1. What other organizations would your facility communicate with (e.g., local law enforcement agencies, your Joint Terrorism Task Force [JTTF], and / or the Federal Bureau of Investigation [FBI])?
	2. Does your facility maintain a relationship with your Department of Homeland Security (DHS) Protective Security Advisor (PSA)?
		1. If so, does your organization have a rapid means of contacting them?
	3. If your facility is covered by Chemical Facility Anti-Terrorism Standards (CFATS), does your organization maintain a relationship with your DHS Chemical Security Inspector (CSI)?
		1. Would your facility notify them of the incident?
	4. Does your organization use Homeland Security Information Network – Critical Infrastructure (HSIN-CI)?
7. Are there counseling services available at your facility for employees who show signs of stress or aggression / violent behavior?
8. What protocols or policies does your facility use to ensure the safety of employees following a known threat from a current or previous employee?
9. Are facility / company policies adequate to de-escalate this scenario from evolving into a violent incident?
	1. In what ways could your facility improve policies, if any?
10. Does your facility use background checks or any screening practices when selecting new employees?
	1. Does your facility update background checks on existing employees?
11. Does the facility have the ability and procedures to limit and / or monitor access of threatening employees to the facility and / or restricted areas?

This page is intentionally left blank.

# Module Two: Incident

## Scenario

## [Insert Location]

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

A few days pass and some employees notice a car in the parking lot that resembles [insert name]’s. Some confusion ensues as [insert name] has not been to work since his meeting with his supervisor, but the employees think nothing more of it and proceed with their day. Lunch time arrives and most employees leave the building to enjoy their break off-property. As they are leaving, the employees notice smoke coming from a vent on the side of the building by the first-floor cleaning closet near the [insert chemical lab]. Alarms go off and automatically notify the [insert local fire department], while witnessing employees dial 911. Security begins evacuation protocol and proceed to direct employees to the designated rally points outside of the building. At this point, flames are seen coming out of the same vent where the smoke was seen. The fire is beginning to engulf the first floor surrounding the chemical lab, providing a difficult environment for security to evacuate all employees in the area.

Minutes pass and local first responders arrive on scene. As firefighters attempt to extinguish the flames, many employees are trying to reach the police to notify them of a new social media post from [insert name] where he claimed responsibility for the attack with specific details about how he did it. In the post, [insert name] shares his beliefs that the company “needed to be taught a lesson.” When authorities search the parking lot, his vehicle can no longer be found. Shortly after, firefighters manage to extinguish the flames, stopping it from reaching the second floor.

## Discussion Questions

1. Do facility incident response plans at your facility (e.g., Site Security Plans, Emergency Action Plans, Emergency Response Plans, or other appropriate plans) contain protocol for responding to and evacuating during a fire?
	1. Does your facility train employees for this type of emergency incident?
		1. Is emergency contact information made available to the call desk?
		2. What procedures exist for sheltering-in-place and evacuation?
		3. What other emergency-related training does your facility offer employees?
	2. What notification systems do chemical facility owners / operators have in place to warn employees both on and off-site during such an incident?
	3. How does your facility communicate with employees during an incident?
	4. What instructions will your facility give to employees (e.g., evacuation, shelter-in-place, lockdown)?
	5. Is there a way for your facility to account for employees (i.e., those who reported for work that day versus those on leave)?
	6. Are there any critical operations of the facility that your organization must secure for safety reasons?
		1. If so, are there procedures in place for doing so in an emergency?
	7. What other life-safety issues should your facility consider?
2. Does your organization have an emergency response team?
	1. Does your facility train the emergency response team to respond to a fire hazard?
	2. Does the emergency response team transfer response duties to local firefighters when the firefighters arrive on the scene?
		1. When and how does the transfer happen?
3. What are your facility’s evacuation procedures for an incident of this type?
	1. Are there existing plans for a mass evacuation?
		1. Who is responsible for activating the evacuation procedures?
		2. Is there a specified rally point for evacuees?
		3. Would weather impact this location?
		4. Are there secondary and tertiary rally points in case the primary point is a part of the incident or evacuees overwhelm it?
	2. What plans or procedures exist to work with access and functional needs populations?
	3. What agencies would implementing an evacuation involve?
		1. What training has been done on evacuation plans?
4. Given the scenario, does your Emergency Action Plan (EAP) include measures for protecting chemicals at your facility?
5. Who is responsible for ensuring the chemical security measures are met?
6. When your organization notifies responders to a similar scenario, do you include information about the chemicals at your facility?
	1. Are first responders aware of what chemicals are at your facility?
	2. Do you know if first responders are able to adequately respond if an attack at your facility impacts those chemicals?
	3. Who else should your facility notify within the first responder community if the attack impacts those chemicals?
7. What security measures does your organization have that are relevant to this scenario?
	1. Is there security on-site at your facility?
	2. If so, how does your facility train security to respond to this type of incident?
	3. What are security personnel’s roles and responsibilities?
	4. Do security personnel and first responders have interoperable radios / communication?
		1. Do plans exist for public and private sector stakeholders to communicate if they cannot communicate via radio?
	5. Upon arrival, can law enforcement clearly identify security?
	6. What types of perimeter security does your facility have (e.g., fences, doors, gates)?
	7. What types of vehicle control checkpoints are present (e.g., barriers, driveways, parking lots)?
	8. Does the public have access to your facility?
8. How does your organization coordinate the emergency response?
	1. Does your facility preemptively provide any incident response plans (e.g., Site Security Plans, Emergency Action Plans, Emergency Response Plans, or other appropriate plans) to first responders in preparation for potential incidents?
		1. If not, how does your facility communicate key information to first responders during the response to an incident?
	2. How do emergency response personnel access the building?
		1. Upon arrival of law enforcement, is there a “go bag” available to them containing desired items such as a facility map / floor plans, access swipe cards, elevator keys, etc.?
	3. Are there any safety concerns for first responders that your facility needs to address (e.g., entering restricted or hazardous areas)?
	4. Have local first responders previously participated in exercises and / or trainings at the facility?
9. How does your facility handle emergency communication?
	1. Are critical telephone calls getting through?
	2. If not, is there an alternate means of communication available?
	3. How will facility owners / operators interact with media representatives and control media access to the facility?
	4. Are there existing procedures to manage the media when they arrive?
	5. Should your facility make additional emergency announcements to the public?
10. Does your facility maintain security technology that can assist law enforcement in response efforts?
	1. Are there access control capabilities at your facility to coordinate entry of first responders, prevent entry of visitors or additional employees, and manage contractors on-site?
	2. Can your facility remotely control access to critical components or activate / deactivate card readers, including the capability to deactivate a specific card?
11. How would your facility conduct the medical response?
	1. Which organizations and agencies are involved in the medical response?
	2. Which organization or agency would have the lead?
	3. Is there a Mass Casualty Plan in place for an event such as this one?
	4. At what point would your facility inform hospitals of the incident?
		1. Who is responsible for contacting the hospitals?
	5. At what point would first responders’ protocols allow medical personnel to enter the scene and begin triage and treatment of the injured?
		1. What challenges would the ongoing evacuation procedures pose to medical personnel’s work?
12. What information or warnings is your facility releasing to the public?
	1. Who is responsible for the initial messaging?
	2. How quickly is your facility releasing information?
	3. What methods is your facility using to distribute information?
	4. What should the content of the messaging be?
	5. Is your facility sending targeted information to businesses or people in the impacted area?
	6. Are other participating organizations providing their own messaging to their employees?
		1. How do employees obtain the information?
		2. How do other participating organizations distribute the message?
		3. Who in your facility is responsible for coordinating information sharing with other private and public sector organizations?
		4. Are there pre-built message templates for different incidents?
13. How do state and local officials coordinate when responding to an incident at the facility?
	1. Does your facility have Memorandums of Understanding or Memorandums of Agreement in place with any local, regional, or state response agencies?
14. How does your facility coordinate response and who maintains decision-making authority when management is not available?
	1. Do your facility’s incident response plans cover the emergency coordination activities described in the module?
	2. Does the security plan or any other plan outline the delegation of authority?
	3. If your organization locks doors to critical facility components, how does law enforcement obtain access?
	4. Does [insert your facility] identify a safe location for people who are evacuating the immediate area?

This page is intentionally left blank.

# Module Three: Recovery

## Scenario

## [Insert Location]

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

With the perimeter secured, police maintain a safe environment outside while firefighters look for any casualties and employees who could not evacuate because of the flames. Firefighters recover [Insert number] casualties, with [insert number] wounded and [insert number] deceased. Upon further clearing, local first responders discover the fire system managed to save the [insert chemical lab], but with the fire starting in the cleaning closet, the system could not prevent the fire from spreading to the offices in the remainder of the first floor. Structurally, the building remains intact; however, everything else on the first floor has been damaged or destroyed in the flames.

Police conduct interviews and ask survivors for information regarding the attack and for proof of the allegation that [insert name] claimed responsibility for the attack. Workers call on leadership within the organization to provide immediate assistance to employees, including mental health services and allowing employees who are willing to resume work from a new location, including their homes.

## Discussion Questions

1. What is the protocol at your facility when personnel must evacuate?
2. How do your current facility emergency plans address the coordination of emergency response personnel at this point in the incident?
3. How will your facility coordinate personnel accountability and communication?
	1. Who at your facility makes a list of the evacuees?
	2. What does your facility emergency coordinator need to consider (e.g., casualties, evacuation routes, hospitals)?
	3. Who at your facility informs family members of employees if they are deceased?
	4. Who at your facility maintains information about what hospitals the wounded were transported to?
	5. How are family members of wounded individuals who were transported to hospitals notified?
	6. What process exists to reunite employees with their belongings that were left behind during the incident?
4. How do employees leave the site if the employee parking lot is a crime scene and cannot be accessed?
5. What is the process to assist law enforcement with victim identification?
6. Where are the pre-determined locations at your facility for the command post and staging area(s)?
7. What is the impact of law enforcement designating the facility, or portions of the facility, an active crime scene?
	1. How will law enforcement coordinate facility issues related to the investigation with owners / operators?
	2. How will your facility address any impediments to operations?
	3. Will law enforcement be able to estimate the time frame required to consider your facility a crime scene?
8. What information sharing mechanisms are in place at your facility that could be relevant for an incident such as this?
	1. What information about this incident would facility owners / operators share with other facilities in their company or sector?
	2. What mechanisms would facility owners / operators use to relay information to federal, state, and local authorities?
	3. How would facility owners / operators expect to receive information from their federal, state, and local officials?
	4. What information about the incident would facility owners / operators share with families of employees and how would this be done?
	5. What processes are in place at your facility to handle misinformation or rumors about how the incident started?
9. How can facility owners / operators prepare to handle public messaging / media in the aftermath of such an occurrence?
10. What business continuity, continuity of operations (COOP), or rapid recovery plans are in place to address a fire at your facility?
	1. What are your facility’s priorities related to continuity and recovery?
11. Are there any potential liability issues from this incident that your facility managers would be addressing at this point?
12. What assistance is available for employees at your facility following event such as this one?
	1. How does your facility communicate information with personnel and families in the days following the incident?
		1. How will your facility coordinate personnel accountability and communication?
	2. Will your facility make counseling for employees and family members available?
	3. Will there be any financial assistance or benefit programs for employees at your facility if the facility is temporarily shut down?
	4. What is the procedure at your facility if injuries received on the job hospitalize an employee?
	5. Is there an existing process at your facility for assisting the family members of a deceased employee?
13. Does your facility have a designated public information officer (PIO)?
	1. If so, are protocols in place for addressing media inquiries?
	2. How does the media receive information about the incident from your organization?
	3. Does your facility’s PIO have pre-built public information templates for use in different kinds of emergencies?
	4. Would your organization use social media during an incident?
14. Following this attack, what additional protective measures will be put into place at your facility or in your community?
	1. How would private and public sector stakeholders obtain information on protective measures?
	2. How and with whom would your facility share any relevant classified information?
	3. How does your facility share relevant information within its critical infrastructure sector?
		1. How does your facility communicate information to other members of its sector or receive information from them?
		2. Does your facility know how to contact its Sector-Specific Agency?
		3. Does your facility have a Homeland Security Information Network (HSIN) account?
	4. Does your facility know how to contact its DHS Protective Security Advisor (PSA)?
	5. Does your facility know how to contact its DHS CSI?
	6. How does your facility protect its employees?
15. What procedures are in place to secure any dangerous chemicals during the recovery process?

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] |
|  |
|  |
|  |

# 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 |
| **CSI** | Chemical Security Inspector |
| **CTEP** | CISA Tabletop Exercise Package |
| **COOP** | Continuity of Operations |
| **DHS** | Department of Homeland Security |
| **EAP** | Emergency Action Plan |
| **EPT** | Exercise Planning Team |
| **FBI** | Federal Bureau of Investigation |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **IP** | Improvement Plan |
| **JTTF** | Joint Terrorism Task Force |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SitMan** | Situation Manual  |
| **SME** | Subject Matter Expert |
| **TTX** | Tabletop Exercise  |
| **USSS** | U.S. Secret Service |

