Chemical Sector Domestic Threat Exercise

Situation Manual

[Insert Date]

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

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

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 8:00 a.m. | 8:30 a.m. | Registration |
| 8:30 a.m. | 8:45 a.m. | Welcome and Introductions |
| 8:45 a.m. | 8:55 a.m. | Exercise Objectives |
| 8:55 a.m. | 10:05 a.m. | Module One: Overseas Attacks and Domestic Threats |
| 10:05 a.m. | 10:20 a.m. | Break |
| 10:20 a.m. | 11:20 a.m. | Module Two: Imminent Threat |
| 11:20 a.m. | 12:00 p.m. | Hot Wash / Closing Comments |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Chemical Sector Domestic 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, and Response [insert other Mission Areas as appropriate] |
| **Capabilities** | Planning; Intelligence and Information Sharing; Risk Management for Protection Programs and Activities; Public Information and Warning [insert additional core capabilities as necessary] |
| **Objectives** | 1. Review intelligence and information sharing, and dissemination processes in relation to a credible threat and / or [insert threat vector] to domestic Chemical Sector infrastructure owners / operators. 2. Assess information sharing capabilities with public sector partners and federal, state, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures. 3. Discuss and identify private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under the National Incident Management System (NIMS) with local, state, and federal agencies. 4. Discuss gaps and challenges in private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident. 5. [Insert additional exercise objectives as necessary]. |
| **Threat or Hazard** | Threat of Terrorist Attack [insert additional threat vector, as necessary] |
| **Scenario** | Multiple executed and attempted terrorist attacks overseas lend credibility to a potential attack on a critical Chemical Sector Facility. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being utilized, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise POC (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

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

For additional information regarding core capabilities, please visit: <https://fema.gov/emergency-managers/national-preparedness/mission-core-capabilities>.

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Review intelligence and information sharing and dissemination processes in relation to a credible threat and / or [insert threat vector] to domestic Chemical Sector infrastructure owners / operators. | * Planning * Intelligence and Information Sharing * Public Information & Warnings |
| Assess information sharing capabilities with the public sector partners and federal, state, local, tribal, and territorial government departments and agencies in accordance with applicable plans and procedures. | * Planning * Intelligence and Information Sharing * Public Information & Warnings |
| Discuss private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident and the coordination activities under NIMS with local, state, and federal agencies. | * Planning * Risk Management for Protection Programs and Activities |
| Discuss gaps and challenges in private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident. | * Planning * Intelligence and Information Sharing * Risk Management for Protection Programs and Activities |
| [Insert objective] | * [Insert capability aligned to each objective] |

Table 1. Exercise Objectives and Associated Capabilities

## Participant Roles and Responsibilities

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

* **Players:** 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: Overseas Attacks and Domestic Threats
* Module Two: Imminent Threat

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: Overseas Attacks and Domestic Threat

## Global Terrorist Attacks

### May 27, 20[XX] – June 5, 20[XX]

Over the course of a ten day period, there are multiple terrorist attacks on critical infrastructure in Africa and Europe and an additional attack is thwarted in Germany. Details of the attacks are as follows:

**May 27, 20[XX]:** There is a water-borne improvised explosive device (WBIED) attack against a U.S.-owned floating production, storage, and offloading (FPSO) vessel located off the coast of Nigeria. The attack results in eight individuals killed and seven injured. Several terrorist organizations claim responsibility for the attacks.

**June 1, 20[XX]:** Two chemical plants in Germany, a coal power plant in Belgium, and oil pipelines in France are attacked with large vehicle borne improvised explosive devices (LVBIEDs), flexible linear shaped charges (FLSs), and explosively formed projectiles (EFPs). In the Germany attacks, 190 tons of chlorine is released causing the evacuation of nearby towns. The four attacks result in approximately 1,000 casualties.

**June 5, 20[XX]:** German authorities thwart an attack against a pipeline in eastern Germany after local residents report suspicious activity near a pipeline pumping station. German law enforcement personnel question numerous individuals and arrest five suspects.

## Discussion Questions

1. How would your facility receive unclassified information regarding the successful attacks on overseas critical infrastructure?
   1. Which, if any, information sharing mechanisms would be used?
   2. What information would your facility require? Who would you contact to obtain this information and how would you contact them?
   3. What should you expect to see, if anything, on the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) portal at this time?
   4. Does your facility have mechanisms in place to share information with international partners? If so, what are the procedures currently in place to do so?

## Scenario Update: Domestic Threats

### June 12, 20[XX] – June 14, 20[XX]

Through ongoing investigations and analysis, a credible threat to domestic critical infrastructure is identified in a specific geographic area of the United States. Upon receipt of additional information and intelligence, law enforcement issues a “be on the lookout” (BOLO) within the community.

Details of the ongoing activities and threat indications are as follows:

**June 12, 20[XX]:** A Drug Enforcement Administration (DEA) informant in Tijuana, Mexico observes and reports a meeting between Malian nationals and high level members of a Tijuana-based drug trafficking organization. A subsequent investigation determines that the Malian nationals have strong financial ties to the international terrorist organization known as “Universal Adversary” (UA).

**June 13, 20[XX]:** A joint investigation of the attacks in Europe and Nigeria provides the following information:

* Two of the individuals captured in Germany likely attended a UA training camp near Tessalit, Mali.
* At least one of the individuals suspected in the Nigerian attacks attended the same camp at the same time as the Germany suspects.
* Analysis of all-source intelligence gained prior to the Belgian attack reveals possible transmission of the “go order” to the suspected Belgian cell leader from a suspected UA safe house in Gao, Mali.
* At least half of the individuals involved in the European attacks were European Union (EU) citizens.

**June 14, 20[XX]:** Intelligence indicates that there is a credible threat to domestic critical chemical infrastructure in the South Central United States with potential targets within [insert your location], Houston; Albuquerque, New Mexico (N.M.); Baton Rouge, Louisiana; and Oklahoma City metropolitan areas.

## Federal Responses

**Department of State (DOS):** The Bureau of Consular Affairs issues a *Consular Information Sheet* to American citizens travelling abroad as there is a credible threat. Since the threat is against a specific facility or sector, DOS Overseas Advisory Council sends the information directly to the targeted organization.

**Department of Justice:** The Federal Bureau of Investigations (FBI) posts available information to InfraGard, and issues an Intelligence Bulletin to appropriate state and local law enforcement.

**Department of Homeland Security (DHS):** DHS / Office of Intelligence and Analysts (I&A) coordinates with the FBI and DHS / Office of Operations Coordination (OPS) to develop and disseminate information, and uses available intelligence to brief the DHS Secretary. CISA coordinates with DHS / OPS to post threat information on HSIN and Technical Resource for Incident Prevention wire (TRIPwire). Additionally, CISA monitors the development of the situation through the National Infrastructure Coordinating Center (NICC), and provides security recommendations, as requested.

## Discussion Questions

1. With a credible threat to domestic critical infrastructure in your specific city, how would you receive unclassified and classified information regarding this threat?
   1. What information would your facility require? Who would you contact to obtain this information? How would you contact them?
   2. Are there processes in place to gather information and further distribute this information internally and, if so, what are those processes?
   3. Are there processes in place to share information with subsidiary facilities in other states or regions?
   4. Would your facility share this information with international partners? What would be the benefit, if any?

## Scenario Update: Domestic Threats Update

### June 15, 20[XX] – June 16, 20[XX]

**June 15, 20[XX]:** A representative from [insert your facility name] in [insert your location] receives a pone call from an anonymous caller, identifying himself as a member of UA.

The caller expresses frustration with U.S. foreign policy, stating that the country will be held accountable. The caller informs the representative that the facility can either pay a submission tax of $3 million to UA or expect “considerable damage” to its facility “soon”. The caller states that they have fulfilled their obligations to offer the facility an alternative to violence. This is the third such threatening call this month to [insert your facility name].

**June 16, 20[XX]:** The [insert your facility name] plant in [insert your location] identifies several suspicious activities within the last several weeks, including a cut fence (although there was no evidence of theft), multiple inquiries of the gate guard, and unknown vehicles parked in and around the facility.

**Later that afternoon:** A Globocon chemical facility located in Albuquerque, N.M. and a Transdom World Enterprises chemical facility in Houston, each receive calls similar to the one received by [insert your facility name]. The caller’s complaints are alike in nature including statements of growing frustration and that the United States must pay. Each caller suggests that his organization was involved with the incidents in Africa and Europe, and that the Globocon and Transdom World Enterprises plants were next.

## Discussion Questions

With a credible threat to the Chemical Sector, what specific actions and/ or protective measures would your facility take in response to the threat information? What avenues are available to your facility to request more details regarding the threat?

If applicable, have you complied with any regulatory or stewardship program requirements or standards?

For all facilities:

What documents guide your facility in a credible threat environment?

Are the documents readily available to everyone with a need to know?

Would you activate specific planning or operational capabilities, to include business continuity plans?

Would you share these specific measures with local, state, and federal partners?

Who makes the call to activate specific planning or operational capabilities, and how quickly is the call made?

If contacted regarding a threat, is there a means in place to gather all pertinent information for possible prevention, mitigation of, or recovery from damages as a result of an attack?

Once a threat is made, are procedures in place to immediately engage facility security?

At what point, and to what degree, do you contact and engage local, state, and federal resources (i.e., local and state law enforcement, fire and rescue, emergency management, and your Protective Security Advisor [PSA])?

With whom are you exchanging intelligence and information?

Are procedures in place to allow emergency onsite access to local rescue and law enforcement personnel?

This page is intentionally left blank.

# Module Two: Imminent Threat

## Scenario

### June 17, 20[XX] – June 20, 20[XX]

Over a four day period in mid-June, significant domestic investigation and analysis activities identify a credible threat to two specific U.S. metropolitan areas and specific critical infrastructure sectors.

The details of the information gathered are as follows:

**June 17, 20[XX]:** DHS / Customs and Border Protection (CBP) detains a foreign national trying to cross the U.S.-Mexico border with falsified identification paperwork. A subsequent investigation leads CBP to believe that he may be one of six foreign nationals listed on a recent law enforcement BOLO.

An analysis of the laptop computer being carried by the detained foreign national leads investigators to believe that infrastructure of the Chemical or Oil and Natural Gas Sectors in [insert your location] and Houston are the most likely targets for attacks.

**June 18, 20 [XX]:** A security officer at the Transdom World Enterprises chemical facility located in Houston discovers what appears to be an explosive device attached to the lower half of a tanker car adjacent to the plant. The local police department (PD) is called and sends in its bomb squad to investigate the threat. Local PD orders the immediate evacuation of the plant and the surrounding areas.

Subsequent investigation by the bomb squad reveals that the device is likely a live improvised explosive device (IED). It is eventually rendered safe.

**June 19, 20[XX]:** [Insert your facility name] and an additional plant in Oklahoma City receive more threatening phone calls, explaining that the bomb found at the Transdom World Enterprises facility yesterday was the first of many to follow. The callers state that all U.S. plants can expect to find similar devices and that this was only the beginning.

## Federal Response

Through the National Terrorism Advisory System (NTAS), the DHS Secretary issues an “imminent threat” alert for the Chemical, Oil, and Natural Gas Sectors in the localities impacted. The DHS Secretary tasks DHS with identifying the impacts of the alert, the cascading effects, and recommended courses of action. DHS provides tactics, techniques, and procedures (TTPs) and other protective recommendations to facilities via HSIN.

## Discussion Questions

1. Based on the credible threat information, and the discovery of the actual device, NTAS issued an “imminent threat” alert.
   1. How would this alert affect your facility?
   2. Based on your regulatory agencies’ mandates, are there any additional actions you would take?
   3. Does your facility await government advisories before taking action?
   4. If / when the alert expires and is not renewed, would you follow suit or maintain posture?
2. Who would be in charge of the situation at your facility? Is this identified in a plan?
3. Given the scenario, does your Emergency Action Plan (EAP) include measures for protecting the security of chemicals at your facility?
4. Who is responsible for ensuring the chemical security measures are met?
5. Given the scenario, does your notification to responders include information about the chemicals at your facility?
   1. Do you maintain a relationship with first responders as to what chemicals are at your facility?
   2. Do you know if they are able to adequately respond if an attack at your facility impacts those chemicals?
   3. Who else within the first responder community should be notified if the attack impacts those chemicals?
6. How would your facility handle the media? Does it have a public relations plan? Does this plan account for elected officials at the state and local level?
7. Are there any procedures at your facility that would have prevented access to the terrorist or domestic criminal within this scenario?
   1. What are they?
8. Does your plan address access control?

## Scenario Update

Later that day, facility employees are inquiring if it is safe to come into work. Enough employees call in sick that production is curtailed.

While attempting to find additional labor, facility management receives a call from a local elected official’s office. The official’s staffer reports that the office received numerous calls from citizens worried about the facility and its proposed expansion, which is under zoning review. The staffer specifically asks what information about the threat they received, from what sources, and what further information they need from the government.

Facing a credible and specific threat, [insert your facility name] must make difficult decisions as complications with physical security, employee security, plant operations, media reports, and local relations become overwhelming.

## Discussion Questions

1. How would employees receive notification of the threat?
2. What procedures, if any, would be used to account for employees onsite and ensure all possible suspects were found?
3. Does your facility have a contingency or continuity of operations plan?
   1. Does it address operations in a reduced staff environment? Are there procedures in place to rectify a loss of staff?
   2. Does it clearly define a line of succession for positions of authority?
4. What would be the impact on production? How would this be determined?
5. What would be the cascading effects locally and / or nationally as a result of production curtailment?
6. Based on your vulnerability assessment and security plan, were you able to determine if your existing plans have gaps? How would you fill those gaps?
7. How would you respond to elected official inquiries?

# 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 was 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 |
| **BOLO** | Be On The Lookout |
| **CBP** | U.S. Customs and Border Protection |
| **CFATS** | Chemical Facility Anti-Terrorism Standards |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CTEP** | CISA Tabletop Exercise Package |
| **DEA** | Drug Enforcement Administration |
| **DHS** | Department of Homeland Security |
| **DOS** | Department of State |
| **EAP** | Emergency Action Plan |
| **EFP** | Explosively Formed Projectile |
| **EPT** | Exercise Planning Team |
| **EU** | European Union |
| **FBI** | Federal Bureau of Investigation |
| **FLS** | Flexible Linear Shaped |
| **FPSO** | Floating Production, Storage and Offloading |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **I&A** | Office of Intelligence and Analysis |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **LVBIED** | Large-Vehicle Borne Improvised Explosive Device |
| **MTSA** | Maritime Transportation Security Act |
| **NGO** | Non-Governmental Organization |
| **NICC** | National Infrastructure Coordinating Center |
| **NIMS** | National Incident Management System |
| **N.M.** | New Mexico |
| **NTAS** | National Terrorism Advisory System |
| **OPS** | Office of Operations Coordination |
| **PD** | Police Department |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **TRIPwire** | Technical Resource for Incident Prevention |
| **TTP** | Tactics, Techniques, and Procedure |
| **TTX** | Tabletop Exercise |
| **UA** | Universal Adversary |
| **WBIED** | Water-Borne Improvised Explosive Device |

