

Chemical Sector Unmanned Aerial System Threat Tabletop Exercise

Situation Manual

[Insert Date]

\*[Insert Caveat]\*

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

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 8:00 a.m. | 8:30 a.m. | Registration |
| 8:30 a.m. | 9:00 a.m. | Welcome and Participant Briefing |
| 9:00 a.m. | 9:45 a.m. | Module One: Intelligence and Information Sharing |
| 9:45 a.m. | 10:00 a.m. | Break |
| 10:00 a.m. | 10:45 a.m. | Module Two: Incident and Response Phase |
| 10:45 a.m. | 11:00 a.m. | Break |
| 11:00 a.m. | 11:45 a.m. | Module Three: Recovery and Business Continuity |
| 11:45 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 Unmanned Aerial System (UAS) 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** | * Economic Recovery * Intelligence and Information Sharing * On-scene Security, Protection, and Law Enforcement * Operational Communications * Operational Coordination * Physical Protective Measures * Planning * Public Information and Warning * Risk Management for Protection Programs and Activities |
| **Objectives** | 1. Examine intelligence and information sharing dissemination processes in relation to a credible threat to domestic Chemical Sector infrastructure, including public messaging protocols. 2. Assess information sharing capabilities with public sector partners; 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 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 involving a UAS. 5. Discuss recovery and business continuity in the wake of a UAS incident, including public messaging protocols. 6. [Insert additional exercise objectives, as necessary] |
| **Threat or Hazard** | Threat from a UAS-Borne Improvised Explosive Device (IED) on Chemical Sector Infrastructure. |
| **Scenario** | An interactive, discussion-based exercise focused on an active threat involving a UAS device at a 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 B.] |
| **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).

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Examine intelligence and information sharing and dissemination processes in relation to a credible threat to domestic Chemical Sector infrastructure, including public messaging protocols. | * Intelligence and Information Sharing * On-scene Security, Protection, and Law Enforcement * Operational Communications * Operational Coordination * Planning |
| 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. | * On-scene Security, Protection, and Law Enforcement * Operational Communications * Operational Coordination * Planning |
| Discuss and identify private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident involving a UAS and the coordination activities under NIMS with local, state, and federal agencies. | * On-scene Security, Protection, and Law Enforcement * Operational Communications * Operational Coordination * Planning |
| Discuss gaps and challenges in private sector stakeholders’ emergency preparedness plans and response procedures to a threat-initiated incident involving a UAS. | * Intelligence and Information Sharing * Planning * Risk Management for Protection Programs and Activities |
| Discuss recovery and business continuity plans in the wake of a UAS incident, including public messaging protocols. | * Economic Recovery * Operational Coordination * Planning |
| [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 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:** 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: Intelligence and Information Sharing
* Module Two: Incident and Response Phase
* Module Three: Recovery and Business Continuity

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: Intelligence and Information Sharing

## Scenario

## [Insert Location]

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



Based upon increased chatter coming from the dark web, the Secretary of Homeland Security, in coordination with other federal entities, issues an “Elevated” Threat Alert through the National Terrorism Advisory System (NTAS), warning of a credible terrorist threat against the United States focusing on chemical sector infrastructure. At this time, there is no specific information that would warrant the release of an “Imminent” Threat Alert. For more information, please see **Appendix A.**

The alert states the threat is from a domestic extremist group in the United States with ties to international terrorist organizations that are focused on populated areas where chemical sector facilities are present. Additionally, the alert indicates that these terrorists are sourcing both commercially available UAS, also known as drones, and precursor materials for IEDs. The alert is to remain in place for three months, ending on [insert Date + 3 months].

## Discussion Questions

1. How would your facility receive unclassified information regarding a potential attack on other Chemical Sector infrastructure?
   1. Which, if any, information sharing mechanisms should your facility use?
   2. What information would your facility require? Who would you contact to obtain this information? How would your facility 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?
      1. Do you have a HSIN account?
   4. Does your company / facility have mechanisms in place to share information with international partners, and if so, what are the procedures currently in place to do so?
2. How would your organization expect to receive an NTAS alert?
3. How does your organization work with local intelligence and information centers / fusion centers?
4. How does your organization’s leadership communicate the NTAS Alert to departments within your organization? What do the department heads do with this information?
5. What types of training does your organization conduct based on general or credible threats?
   1. Does your organization conduct any specific training regarding the threat posed by drones?
6. How does your organization share this information with the external stakeholders? What do external stakeholders do with this information?
7. How does your organization share this information with other organizations near your facility? What do these organizations do with this information?
8. How would your actions change if the threat was specific to chemical facilities in your state?
   1. How would your actions change if the threat was specific to your facility?
   2. What specific measures would be taken at your facility to increase its security posture at this time, if any?
9. Are there any other stakeholders outside your organization that you would need to notify based on this information and, if so, who?
10. What kind of messaging, if any, would your organization release to the public?

## Scenario Update: Credible Threat

## [Insert Location]

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

Law enforcement in a neighboring state are investigating a recent break-in at a commercial UAS manufacturer that produces heavy-lift UASs. The stolen UASs possess long-range flight capabilities with attachments that allow the UASs to deliver products remotely. They are also equipped with a solar powered battery that can recharge itself during daylight hours allowing the UAS to achieve a longer than normal flight time.

Through ongoing investigations and analysis, law enforcement determined that a credible threat to Chemical Sector infrastructure is identified in [insert specific geographic area] of the United States near [insert area closest to your location]. Intelligence indicates that domestic terrorists with ties to international terrorist groups are targeting your facility due to the production of chemicals that are used in a wide range of applications.

In conjunction with these developments, there is also an increase in chatter picked up by federal authorities regarding the buying and selling of various materials that, when combined, can be used to create homemade IEDs. Upon receipt of this additional information and intelligence, law enforcement has issued a “Be on the Lookout” (BOLO) within your community requesting anyone who notices suspicious drone activity to report it to local law enforcement.

## Discussion Questions

1. With a credible threat to the Chemical Sector 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 established processes to share information with subsidiary facilities in other states or regions?
   4. Would your company / facility share this information with domestic and / or international partners? What would be the benefit of sharing this information, if any?
2. With 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. What documents guide your company / facility in a credible threat environment?
   2. Is the document readily available to everyone with a need-to-know?
   3. Would your facility activate specific planning or operational capabilities to include 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?
3. If contacted regarding a threat, are there established procedures to gather all pertinent information for possible prevention, mitigation, or recovery from damages as a result of an attack?
   1. Once a threat is made, are procedures in place to immediately engage facility security?
   2. At what point, and to what degree, does your facility contact and engage local, state, and federal resources (i.e., local and state law enforcement, fire and rescue, emergency management, and CISA Protective Security Advisor [PSA])?
      1. With whom is your facility exchanging intelligence and information?
      2. Are procedures in place to allow emergency on-site access to local rescue and law enforcement personnel?
4. What steps would your organization take to mitigate a threat from a UAS attack?
   1. Do your security personnel have experience in dealing with or containing an airborne threat, such as a UAS?
5. What are the prevention and mitigation incident response procedures your facility’s security and emergency response plans mandate?
6. What communication plans are in place to brief employees of the potential hazards from a UAS attack on one of your facilities?
7. What communication plans are in place with neighboring businesses / organizations if there is a UAS sighting?
8. How does your facility integrate UAS detection capability into your emergency operations center (EOC) to ensure synchronization of response effort?
9. What actions would your organization take upon receiving reports of a UAS sighting?
10. How would your facility respond if a threat to your facility is made known to the public?
    1. What type of public relation protocols are in place to address concerns the media may circulate?
    2. What type of public relations protocols are in placed to ensure the neighboring community of the safety of your facility?
    3. As the public inevitably posts information on social media, how does your organization mitigate any potentially misleading information?
11. Who are the law enforcement entities that will receive the UAS sighting report?
    1. What information will you gather on the aircraft (i.e., markings, size payload), potential operator location, and speed / altitude / vector information?
    2. Who will maintain visual contact of the UAS?

# Module Two: Incident and Response Phase

## Scenario

## [Insert Location]

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

It is a windy day with potential rain in the forecast later in the day. As the morning and evening shift workers begin their standard change over routines, several workers outside notice [insert number of UASs / drones] small objects flying closer to their location. As the objects get closer, workers realize the objects flying towards them are drones. Several workers return inside to alert management while others remain outside recording the drones with their cell phones.

As more people make their way outside to observe the drones, the drones begin to fly around different locations of the factory with some hovering over storage tanks holding [insert type of chemical]. None of the workers notice that each drone appears to be carrying a misshapen package with wires leading to a cell phone. Within a few minutes, the drones suddenly explode, causing panic as some of the workers attempt to flee the area. Some workers are running away from the facility while others run inside to alert the rest of the workers inside the facility. As each drone detonates, secondary explosions occur and create chemical spills in various areas.

Employees’ preliminary reports state [insert number] people were killed or injured in the explosions and [insert number] people were injured while fleeing the scene and exposed to toxic chemicals. Reports of multiple explosions at your location are starting to show up in the news and various social media platforms.

## Discussion Questions

1. What protocols are in place to alert your facility staff of this type of incident?
   1. Who is responsible for sending out the alert or warning?
2. Do any standard operating procedures (SOPs) include roles and responsibilities for your facility staff?
3. Are there contingency plans in place in case someone cannot fulfill these roles and responsibilities due to an injury or death?
4. Does your facility have an Emergency Response Team? If so:
   1. Does your organization train the Emergency Response Team to respond to this type of event?
   2. What type of capabilities does the team have on-site to respond to this event?
   3. Does your facility have medical capability on-site to triage casualties?
5. What level of security would be on site?
   1. How does your facility train security to respond to this type of incident?
6. What are the evacuation procedures for this type of situation?
   1. Who is responsible for activating the evacuation protocols?
   2. Does your facility specify a location for evacuees?
      1. Would your facility change this evacuation location in the event of inclement weather?
      2. Would your facility change this evacuation location because of a chemical spill?
      3. Are there secondary and tertiary rally points in case the primary point is a part of the incident or overwhelmed by evacuees?
   3. Does your facility train staff members in the evacuation procedures?
   4. How does your facility inform staff of the evacuation procedures / plan once the plan is activated?
   5. Are local first responders familiar with your emergency procedures?
7. What type of protocols are in place to maintain accountability of your employees during evacuation procedures?
   1. How would your organization address accountability of your employees in the event standard evacuation procedures are unable to be followed?
8. In the event of an emergency, are there procedure in place to ensure that your organization can shut down chemical processing in an effective and efficient manner?
   1. Can your organization shut down the chemical process without endangering on-site personnel?
9. What on-site hazardous materials (HAZMAT) procedures are in place to mitigate a chemical spill during an emergency?
   1. How would your facility communicate these procedures to the first wave of first responders?
   2. Does your facility possess the necessary equipment, such as fully encapsulating chemical protective (FECP) suits and other personal protective equipment (PPE), to safeguard employees and / or first responders who would be tasked with addressing a chemical spill?
10. What command and control considerations would your facility take at this point in the response?
11. What procedures your facility take to stand up an EOC?
12. Who is responsible for notifying state or federal agencies of the incident, and at what point in the incident would this occur?
    1. What resources or actions would your facility expect from state or federal agencies?
13. How would arriving state and federal resources integrate into the command structure and at which locations (i.e., unified command, area command, EOC, Multiagency Coordination [MAC] Group, etc.)?
14. What is the role of private sector stakeholders in this command structure?
    1. Are private sector stakeholders trained on incident command procedures?
    2. Does your organization have representation within the EOC or the Unified Command?
15. How would law enforcement conduct the response and address the threat?
    1. Which agencies are involved in the response to the IED threat?
    2. Which agency would have the lead in the IED response?
    3. How would law enforcement respond to the reports of an IED?
    4. How would the response change if and / or when the IED was found?
    5. Are there any additional agencies or resources your organization needs to address an IED?
    6. Are there any law enforcement SOPs that would affect other entities (i.e., moving fire / emergency medical services [EMS] out of an IED blast radius after the explosive is discovered, or potentially taking over nearby businesses for command posts or sniper positions)?
    7. How would your organization resolve the IED threat?
16. How would your organization conduct the medical response?
    1. Does [insert your facility name] have a medical cadre trained to respond to this kind of event?
    2. Which organization and agencies are involved in the medical response?
    3. Which organization or agency would have the lead in the medical response?
    4. Is there a Mass Casualty Plan in place for this type of incident?
    5. At what point would your organization inform hospitals of the incident?
       1. Who is responsible for contacting the hospitals?
17. How would your organization or business distribute messaging to your employees?
    1. Would your organization coordinate the messaging with any other businesses?
    2. Does your organization have an identified Public Information Officer (PIO)?
       1. If so, does your PIO have any experience working with other organizations’ or first responder PIOs?
18. How would your facility handle the media?
    1. How quickly is your organization releasing messages to the public?
    2. Who is responsible for this type of messaging?
    3. How is your organization releasing the messages?
    4. How does your organization coordinate messages across the different agencies and organizations?
19. Would anything delay fire and emergency medical services personnel from entering the scene to assist injured participants?
20. Are local law enforcement, fire, and emergency medical services personnel familiar with the physical layout of your facility?
21. How is your organization tracking patients?
    1. Who is responsible for tracking patients?
    2. What is your organization telling families of victims?
22. What actions are local, state, and federal law enforcement agencies taking at this point?

# Module Three: Recovery and Business Continuity

## Scenario

## [Insert Location]

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

The explosions resulted in various levels of structural damage and the destruction of multiple chemical storage units. [Insert your facility] contained the chemical spills and leaks that occurred because of the explosions .

There was a total of [insert number] fatalities as a result of the UAS attack with an additional [insert number] victims sustaining various levels of injuries from the attack and ensuing exposure to chemicals released from the explosions. Local medical facilities are busy treating those who sustained injuries during the attack with [insert local Fire and EMS department] transporting some individuals to medical facilities outside of the area to receive specialized treatment because of the severity of their injuries. Federal and local law enforcement agencies completed their investigation and your facility is no longer a crime scene.

Families continue to try to work through the grieving process for lost loved ones and take care of those who survived the attack. Media is continuing to contact a variety of organizations looking for any additional information. As journalists continue to report on the incident, accounts of the event also continue to circulate on social media.

## Discussion Questions

1. How can owners / operators and government officials prepare to handle the public messaging / media in the aftermath of such an occurrence?
   1. Does your media plan include incidents such as these?
   2. Have your local PIOs had the opportunity to collaborate with other supporting organizations’ PIOs during a crisis?
   3. What is the plan to handle the significant media attention from national and international outlets?
   4. How will your organization restore public confidence?
   5. How will your organization counter potential misinformation?
   6. How will your organization respond to media requests (written notices, press conferences, interviews, etc.)?
   7. Is someone in your organization monitoring social media to maintain awareness of information spreading that may not be accurate?
      1. Who is responsible for monitoring social media for inaccurate information?
      2. What procedures are in place to counter false information on social media?
2. What steps does your organization need to take to ensure the area is cleared of threats?
3. What is the process to collect evidence that belongs to citizens (cell phone videos, cameras, security footage from private businesses, etc.)?
4. What systems exists to reunite personal items with their owner if left at the scene?
5. Following this attack, what additional protective measures will be put into place at your organization or in your community?
   1. How would your organization obtain information on protective measures?
   2. How would your organization share any relevant classified information?
   3. 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)?
   4. Do you know how to contact your CISA PSA?
   5. If you are a CFATS covered facility, do you know how to contact your CISA Chemical Security Inspector (CSI)?
6. Does your organization or business have a continuity of operations plan?
7. What are the priorities for your facility post-incident?
   1. Do your plans, policies, or procedures specify these procedures?
   2. How does your organization communicate these priorities internally?
   3. Does your organization coordinate priorities with county emergency management?
   4. Does your organization coordinate priorities with state or federal agencies?
8. How does your facility determine the status of your facilities before, during, and after an incident?
9. Are there contracts in place to assist in the cleanup of the area prior to reopening?
   1. What type of procedures are in place to address environmental concerns from a chemical spill?
10. Does your organization have established contracts to assist in the reconstruction of damaged areas prior to reopening?
11. What are short-term recovery procedures for your organization or business?
    1. What resources is your organization considering to assist in short-term recovery?
    2. What are the response priorities at this stage of recovery?
    3. What procedures are in place to secure any remaining dangerous chemicals during the recovery process?
12. Who makes the decision on when the facility will be reopened?
    1. What impact would the incidents have on future business deals?
    2. Would other businesses be likely to support your organization again despite these incidents?
    3. How would you organization communicate the decision to reopen to the public and the media?
13. What would the financial impact be on your organization if it was closed because of such an incident?
14. Does your organization or business have employee assistance services (financial, medical, mental health, etc.) available for your employees?
    1. How would your organization communicate available services to your facility’s employees?
    2. What plans are in place to support employees if your facility is unable to open for an extended period?
    3. What if some employees are incapable of returning to work because of the psychological or physical trauma?
    4. Does your facility have an SOP for visitors or outside contractors that were impacted by the incidents?
15. At what point would you consider the area and all associated organizations or businesses stabilized and back to steady state?
    1. Who determines when it is safe for employees, visitors, and outside contractors to return to the area?
    2. How does your facility communicate to the public that it is returning to steady operations?

## Scenario Update: Credible Threat

## [Insert Location]

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

Several weeks have passed since the attack. [Insert your facility’s name] replaced the various chemical storage units that were destroyed or damaged during the attack. [Insert your facility’s name] repaired the structural damage incurred along with other damages. New chemicals and other resources were shipped in to replenish resources that were lost because of the attack. Federal, state, and local authorities inspected [Insert your facility’s name] with each giving your facility the green light to reopen.

With the facility ready to reopen, many of your employees are ready to return to work; however, there are some employees and local members of the community who express reservation regarding reopening the factory. Numerous concerns from public safety, safety of your facility’s employees, and impact to the environment are topics that members of the community and employees wish to address.

## Discussion Questions

1. Does your company / facility have a long-term contingency or continuity of operations plan?
   1. Does the plan address operations in a reduced staff environment? Are there procedures in place to rectify a loss of staff?
   2. Does the plan clearly define a line of succession for positions of authority?
   3. Would your company / facility conduct a vulnerability assessment in this scenario? Why or why not would your facility conduct a vulnerability assessment?
      1. If so, based on your vulnerability assessment and security plan, would your facility be able to determine if your existing plans have gaps? How would you fill those gaps?
2. What procedures, if any, would be used to ensure an event like this does not happen at your facility again?
   1. Has your facility reevaluated security procedures since this incident to ensure an event like this does not occur again?
3. How would employees receive notification that they are able to return to work?
4. How would your organization encourage employees to return after such an incident?
5. How would your organization address concerns from the local community regarding public safety?
6. How would your organization address environmental concerns from both employees and the local community?
7. What procedures are in place to address any long-term impacts that may result from the spilling of hazardous materials?
8. What would be the impact on chemical production? How would your organization determine this impact?
9. What would be the cascading effects locally and / or nationally as a result of production curtailment?
10. 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?
11. What type of community outreach does your organization have to ensure the local community that it is safe to reopen and operate your facility?
12. What type of public relations campaign do you have in place for other communities that your organization operates in to ensure that your facilities are safe?
13. How does these incidents impact future operations?
    1. How will your company address lessons learned from this incident into their EOP?
    2. Will your organization share this learned lessons with industry partners and others in the chemical sector to establish best practices and new SOPs to address events such as this?
14. How will you respond to inquiries from elected officials?

This page is intentionally left blank.

# Appendix A: Sample National Terrorism Advisory System Alert

This image is a sample of a National Terrorism Advisory System Alert. The sample alert reads: 

HEADER: National Terrorism Advisory System ALERT
Date & Time Issued: [Month] [Day], 20XX 

SUMMARY: Based on recent intelligence gathering efforts, the Department of Homeland Security is issuing an Elevated Threat alert for the Chemical Sector. 

DURATION: [Month] [Day], 20XX 12:00 PM - [Month] [Day], 20XX, 11:59 PM

DETAILS: 

The Department of Homeland Security in consultation with the Federal Bureau of Investigation has reviewed newly gathered intelligence and has deemed there to be a credible threat against the Chemical Sector. 

Current intelligence indicates that an attack could be focused on chemical manufacturing facilities, using Unmanned Aerial System (UAS) and Improvised Explosive Devices (IED)

Authorities are currently investigating a number of domestic extremist groups in the United States who are sourcing precursor materials for IEDs. 

Local law enforcement authorities are encouraged to work with their private sector partners to ensure they are aware of the Elevated Threat status. 

AFFECTED AREAS: Current intelligence focuses the threat on Chemical Sector facilities in the United States 

HOW YOU CAN HELP: The public can assist authorities by reporting any suspicious activity they see. To report suspicious activity, the public should contact their local law enforcement agency and describe specifically what was observed: who or what you saw, when you saw it, where it occurred, and why its suspicious. 

BE PREPARED: The public should ensure they are aware of their surroundings during daily operations at chemical facilities. 

STAY INFORMED: DHS NTAS website: http://www.dhs.gov/alerts and http://twitter.com/NTASAlerts
https://dhs.gov/see-something-say-something

FOOTER: 
If you see something, say something. Report suspicious activity to local law enforcement or call 911. 

The National Terrorism Advisory System provides Americans with alert information on homeland security threats. It is distributed by the Department of Homeland Security. More information is available at www.dhs.gov/alerts. To receive mobile updates: www.twitter.com/NTASAlerts


This page is intentionally left blank.

# Appendix B: 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 C: Relevant Plans

[Insert excerpts from relevant plans, policies, or procedures to be tested during the exercise.]

This page is intentionally left blank.

# Appendix D: Acronyms

| Acronym | Term |
| --- | --- |
| **AAR** | After-Action Report |
| **BOLO** | Be on the Lookout |
| **CFATS** | Chemical Facility Anti-Terrorism Standards |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CSI** | Chemical Security Inspector |
| **CTEP** | CISA Tabletop Exercise Package |
| **EMS** | Emergency Medical Service |
| **EOC** | Emergency Operations Center |
| **EPT** | Exercise Planning Team |
| **FECP** | Fully Encapsulating Chemical Protection |
| **HAZMAT** | Hazardous Materials |
| **HSIN-CI** | Homeland Security Information Network – Critical Infrastructure |
| **IED** | Improvised Explosive Device |
| **IP** | Improvement Plan |
| **MAC** | Multiagency Coordination |
| **MTSA** | Maritime Transportation Security Act |
| **NIMS** | National Incident Management System |
| **NTAS** | National Terrorism Advisory System |
| **PIO** | Public Information Officer |
| **POC** | Point of Contact |
| **PPE** | Personal Protective Equipment |
| **PSA** | Protective Security Advisor |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedure |
| **SSA** | Sector-Specific Agency |
| **TTX** | Tabletop Exercise |
| **UAS** | Unmanned Aerial System |

