[Insert Cover Picture]

Food Manufacturing Facility Tabletop Exercise

Situation Manual

[Insert Date]

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

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

This page is intentionally left blank.

# Exercise Agenda

| Start Time | End Time | Activity |
| --- | --- | --- |
| 7:45 a.m. | 8:30 a.m. | Welcome and Introductions |
| 8:30 a.m. | 9:15 a.m. | Module One: Pre-Incident Information Sharing |
| 9:15 a.m. | 9:30 a.m. | Break |
| 9:30 a.m. | 10:30 a.m. | Module Two: Incident Response |
| 10:30 a.m. | 10:45 a.m. | Break |
| 10:45 a.m. | 11:45 a.m. | Module Three: Recovery |
| 11:45 a.m. | 12:00 p.m. | Hot Wash / Closing Remarks |

*\*All times are approximate*

This page is intentionally left blank.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Food Manufacturing Facility Tabletop Exercise (TTX) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This exercise is a TTX, planned for four hours 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 * Environmental Response / Health and Safety * Infrastructure Systems * Intelligence and Information Sharing * Interdiction and Disruption * Operational Communications * Operational Coordination * Physical Protective Measures * Planning * Public Information and Warning * Risk and Disaster Resilience Assessment * Risk Management for Protection Programs and Activities * Situational Assessment * Threats and Hazards Identification * [Insert additional capabilities as necessary] |
| **Objectives** | 1. Discuss information sharing procedures and communication and coordination protocols between private and public sector partners. 2. Identify organizational risk factors and examine emergency response plans for addressing a potential threat at a food manufacturing facility. 3. Examine business continuity and recovery plans and procedures following a chemical contamination in a food manufacturing facility. 4. [Insert additional exercise objectives as necessary] |
| **Threat or Hazard** | The malicious introduction of chemicals of interest (COI) into a food manufacturing production chain. |
| **Scenario** | This TTX focuses on an insider attack at [Insert Name] food manufacturing facility. The scenario consists of three modules: Pre-incident Information Sharing, Incident Response, and Recovery. |
| **Sponsor** | [Insert the name of the sponsor organization, as well as any grant programs being used, if applicable] |
| **Participating Organizations** | [Please see Appendix A.] |
| **Point of Contact** | [Insert the name, title, agency, address, phone number, and email address of the primary exercise point of contact (POC) (e.g., exercise director or exercise sponsor).] |

# General Information

## Exercise Objectives and Capabilities

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

| **Exercise Objectives** | **Capability** |
| --- | --- |
| Discuss information sharing procedures and communication and coordination protocols between private and public sector partners. | * Intelligence and Information Sharing * Operational Communications * Operational Coordination * Planning * Public Information and Warning * Situational Assessment |
| Identify organizational risk factors and examine emergency response plans for addressing a potential threat at a food manufacturing facility. | * Environmental Response / Health and Safety * Infrastructure Systems * Interdiction and Disruption * Operational Communications * Operational Coordination * Physical Protective Measures * Risk and Disaster Resilience Assessment * Risk Management for Protection Programs and Activities * Threats and Hazards Identification |
| Examine business continuity and recovery plans and procedures following a chemical contamination in a food manufacturing facility. | * 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 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: Pre-Incident Information Sharing
* Module Two: Incident Response
* 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: Pre-Incident Information Sharing

## Scenario

## [Insert Location]

### [Insert Month, Day, Year]: 8:10 p.m.

[Insert Facility Name] is a [insert product(s)] manufacturing facility in [insert location]. On [insert date], company security personnel identify several posts on social media platforms from individuals threatening the company, specifically its manufacturing facilities. Based on the comments and posts, investigators suspect one of the individuals may be a former employee with knowledge of the facility.

Several of the posts call for violence against the company, and some comments express sympathy and encourage other workers to get involved. At this time, security personnel cannot verify the legitimacy of this threat but will keep the investigation open. Employees will begin arriving at the facility in under 12 hours to begin their shifts.

## Discussion Questions

1. How would your organization expect to receive credible threat information?
   1. Does your organization conduct any social media monitoring?
      1. If so, how does the monitoring team disseminate that information to the leadership team?
   2. Does your organization use any threat detection services?
2. What are your organization’s priorities upon notice of a credible threat?
   1. Does your organization have security or screening systems prior to entering the facility?
   2. Would your security posture change upon knowledge of a credible threat?
3. How does your agency triage the information you receive (formal reporting, hearsay, social media, etc.)?
4. What formal information sharing processes would your organization use at this point?
   1. Would your organization send out messages to employees? The public?
   2. Would your organization send out any messaging for non-credible threats?
5. What resources does your organization use to disseminate information?
   1. What notification capabilities (e.g. alerts, email, telecom, text message, etc.) does your organization use to share information and communicate protective measures?
6. What measures would law enforcement take at this time to protect your organization?
7. How is your organization coordinating with information sharing partners, such as the Federal Bureau of Investigation (FBI), fusion centers, and local law enforcement?
8. Does your organization or agency conduct any specific trainings based on credible threats?
9. What plans exist describing the required protective measures your organization will take upon a potential threat?
10. What protocols or policies does your organization use to ensure the safety of employees following a known threat from a current or previous employee?
    1. Do these policies include information and protocols for addressing destructive behavior, such as theft, vandalism, and sabotage?
    2. Do employees know who to contact with questions and concerns relating to insider threats?
    3. Is there a system for reporting signs of potentially aggressive / violent behavior in the workplace?
    4. Is there a way for employees to report non-violent suspicious behavior?
11. What additional notifications does your organization need to distribute outside of your organization?
12. How does your organization screen potential employees prior to hiring? Are there processes to remove facility access to individuals who are no longer employed by your organization?

# Module Two: Incident Response

## Scenario

## [Insert Location]

### [Insert Previous Date + 2 Days]: [Time]

Several days after security personnel discovered the social media threats, protective measures at [Insert Name] facility remain enhanced, but no one else has reported suspicious activity. Facility production is functioning in a “business-as-usual” capacity. At 2:15 p.m., during routine quality control / quality assurance (QC / QA) checks, an employee finds a foreign substance in a batch of product. The employee who discovered the contamination notifies their manager, and [Insert Facility or Facility Manager] immediately halts the production line for investigation.

Upon further testing, the investigation uncovers that someone introduced a COI to the product, rendering it dangerous for consumption. Investigators search the facility, and at 3:30 p.m. find canisters of a liquid COI underneath a station on the production line. The investigation team conducts an inventory of COIs and discovers that an individual took the canisters from a storage room inside the facility. There is no evidence of forced entry into the locked storage space.

At 4:05 p.m., the QC / QA department verifies the chemicals found in the product match those found under the production line. QC / QA professionals deem all the product from that batch toxic and require their disposal. Yesterday and throughout today, numerous trucks left the facility to deliver product to distribution centers throughout the region. Thorough testing of earlier batches ensues to determine when the unidentified individual first introduced COI to the product, but the investigation is still ongoing.

## Discussion Questions

1. What would be your organization’s immediate priorities upon learning of this type of contamination?
2. What type of formal plans or procedures exist that outline needed actions and responsibilities to respond to an incident like this?
3. What procedures exist for initiating a response to this type of incident?
   1. How does your organization coordinate response and who maintains decision-making authority?
   2. What procedures exist to quickly stop production in your facility?
   3. At what point, if any, does your organization notify local authorities of an incident?
4. What are your organization’s standard operating procedures (SOPs) for roles and responsibilities related to investigating production line issues regarding food safety?
   1. Who is responsible for leading this type of investigation?
5. How does your organization train employees to respond to such an incident?
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 you communicate with (e.g., local law enforcement agencies or the FBI) regarding this incident?
   2. What is your organization’s relationship with your Department of Homeland Security (DHS) Protective Security Advisor (PSA)? How would you contact them?
   3. Does your organization use the Homeland Security Information Network—Critical Infrastructure (HSIN-CI) portal or similar information-sharing network?
7. Upon confirmation of a foreign substance in the product, what procedures are there for ensuring the safety of consumers?
   1. How does your organization coordinate with distribution centers and stores to track and halt potentially contaminated product from reaching consumers?
   2. How does your organization communicate issues with a product to consumers?
8. Does your organization have SOPs related to investigating a sabotage on the production line?
   1. What actions are local, state, and federal law enforcement taking at this point?
   2. How does your organization train security to respond to this type of incident? What are their roles and responsibilities?
9. What security technology does your facility have that can assist an investigation in response efforts?
   1. Does your organization use passcodes or key cards to access restricted areas? Is the security team able to access entry records?
   2. Can security personnel assist in locating suspects via closed-circuit television or similar capabilities?
10. What role would on-site security play in this process?
    1. What would be security’s role upon report of a theft?
    2. What would be security’s role upon report of a poisoning?
    3. How would security coordinate with law enforcement in the described scenario? What would be security’s role both prior to and after law enforcement’s engagement?
11. How does your organization handle public communication?
    1. How will your organization interact with media representatives?
    2. What type of information should your organization share with the public, if any, at this point?

## Scenario Update

### [Insert 12 Hours Post-Incident]

Investigators have identified the individual with access to the storage room who stole the COI. Upon questioning, the employee admits to having posted some of the sympathizing comments on social media that month. Law enforcement believes this individual may have been working with other employees or former employees. The security team has shared its intel with local authorities who are triaging information and looking for other possible accomplices. The facility has not reopened, and authorities deemed the production line a crime scene.

## Discussion Questions

1. What safety requirements does your organization need to meet prior to reopening the facility?
   1. Once met, how would your organization communicate to employees and the public that the facility can safely function?
2. How would your organization communicate with employees following the facility’s closure?
   1. What employee assistance can you provide to employees while they are not working?
3. How long can your organization remain closed while dealing with this incident?
   1. What is the financial impact on your organization during the time it is closed?
4. What local, state and / or federal resources would your organization request?
5. What messaging is your organization sharing with the media at this time?
   1. Do your organization’s SOPs discuss handling misinformation from news or social media outlets?
   2. How would your organization handle incoming requests for information over the phone?
6. How would your organization’s security posture change in the hours and days immediately following this incident?
7. How long would you expect your facility to be shut down following such an incident?
   1. How would this closure impact your organization and employees?
   2. What formal plans or policies exist, if any, for ensuring business operations can resume quickly?

This page is intentionally left blank.

# Module Three: Recovery

## Scenario

## [Insert Location]

### [Insert date, 5 days post-incident: [Insert time]

Five days after your organization found COI in the product, production at the [Insert name] food manufacturing facility has resumed after [insert company personnel] thoroughly investigated and cleaned the production area. [Insert facility] recalled and properly disposed all food produced 48 hours prior to the incident to ensure public safety.

Following their investigation, local law enforcement has arrested three employees responsible for the attack. During questioning, the three employees admitted to posting the social media posts, contaminating the product with COIs during the QC / QA phase, and falsifying QC / QA reports.

There has been extensive national media coverage of the incident due to the widespread recall campaign following the contamination of the product. Vendors nationwide removed the product from their shelves and distribution centers disposed all product in their facilities as a safety precaution.

Misinformation on social media has led to rampant panic and anger, as many people fear that other products from the facility may be contaminated as well. Additionally, some employees indicated that they will not be returning to work because of health concerns.

## Discussion Questions

1. Does your organization have a business continuity, continuity of operations, or rapid recovery plan that addresses this type of incident?
   1. Does it include a crisis communications plan?
   2. What are the short-term recovery objectives for your organization?
2. What resources is your organization considering to assist in short-term recovery?
   1. How would your organization measure these resources?
   2. What local, state, or federal resources are available to assist in recovery or business continuity?
3. How does your organization plan to handle public messaging / media in the aftermath of such an incident?
   1. Who is responsible for coordinating appropriate recall information to the public?
      1. How will this person disseminate this information?
      2. What information does your organization convey to the public at this time? How is this done?
   2. How will your organization resolve potential misinformation?
   3. Is your organization monitoring social media for the spread of information that may not be accurate?
      1. Who is responsible for monitoring social media for inaccurate information concerning the incident?
      2. What procedures exist to counter false information on social media?
4. How is your organization managing potential impacts to your brand and / or reputation?
5. How does this attack change your organization’s security posture?
   1. Would your organization establish any additional security measures surrounding COIs? If so, what would they be?
   2. Would your organization make any changes to employee screenings? Would you conduct more in-depth background checks?
6. What is your comprehensive food defense plan?
   1. How does it address sabotage or other internal threats and hazards?
   2. Are your employees aware of the specifics of this plan?
7. What are your organization’s protocols for regular vulnerability assessments?
   1. Following the incident, would you re-examine them?
8. What are your current protocols for QC / QA?
   1. Following such an incident, would your organization make any changes to the structure of your QC / QA department?
9. What protections exist to shield your organization from litigation after an incident such as this one?
10. At what point would your organization consider the situation “normalized”? Who makes that decision?

# 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 |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **COI** | Chemicals of Interest |
| **CTEP** | CISA Tabletop Exercise Package |
| **DHS** | Department of Homeland Security |
| **EPT** | Exercise Planning Team |
| **FBI** | Federal Bureau of Investigation |
| **HSIN-CI** | Homeland Security Information Network- Critical Infrastructure |
| **IP** | Improvement Plan |
| **POC** | Point of Contact |
| **PSA** | Protective Security Advisor |
| **QC / QA** | Quality Control / Quality Assurance |
| **SitMan** | Situation Manual |
| **SME** | Subject Matter Expert |
| **SOP** | Standard Operating Procedures |
| **TTX** | Tabletop Exercise |
| **USSS** | U.S. Secret Service |

