Food Defense Preparedness and Recall Exercise Package (FD-PREP)



**United States Department of Agriculture**

Controller/Facilitator Handbook

[Date]

The Controller/Facilitator (C/F) Handbook outlines the roles and responsibilities of controllers and facilitators. It also describes the procedures they should follow. Since this handbook contains information about the scenario and exercise administration, it should not be shared with exercise players. It should only be shared with controllers or facilitators.

Please note that all the information on the following pages may not apply to all exercises that may be conducted using this toolkit. Exercise leaders may adapt the instructions to their situation, if needed. This document contains a lot of detail in order to accommodate entities planning to conduct exercises with a large number of participants, or that may wish to seek Federal or State funding.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Food Defense Preparedness and Recall Exercise Package (FD-PREP) |
| **Exercise Dates** | [Indicate the start and end dates of the exercise] |
| **Scope** | This is a tabletop exercise planned for 60-90 minutes. It is meant for FSIS-regulated establishments or others who wish to test food defense plans or practices. |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response, Recovery |
| **Core Capabilities**  (As defined by the U.S. Department of Homeland Security) | **Choose Capabilities you want to test in this exercise:**  Planning  Operational communications  Situational assessment  Public information and warning  Operational coordination  Intelligence and information sharing  Screening, search, and detection  Access control and identity verification  Physical protective measures  Cyber security  Risk management for protection programs and activities  Supply-chain integrity and security  Long-term vulnerability reduction |
| **Objectives** | Test your food defense plan  Test your food defense practices  Test your recall plan  Test your response and recovery plans  Test your cyber security practices |
| **Threat or Hazard** | Intentional adulteration of meat, poultry, processed egg products, and fish of the order Siluriformes. |
| **Scenario** | **Choose a scenario. Estimated time to complete each scenario is 60 – 90 minutes.**  Settling the Score – A recently terminated employee adulterates your establishment’s product.  Virtual Outrage – Your establishment’s automated control systems are locked down by ransomware.  Smooth Operator – Your establishment’s reputation is at risk after an activist group spreads a malicious video.  Road Rage – Your establishment faces losses after theft of product and suspected contamination by an imposter transport contractor. |
| **Sponsor** | [Insert the name of the sponsor organization and any grant programs being utilized, if applicable] |
| **Participating Organizations** | [Insert a brief summary of the total number of participants and participation level (i.e., establishment personnel, observers, others). Consider including the full list of participating agencies in Appendix B.] |
| **Point of Contact** | [Insert the name, title, address, phone number, and email address of the primary exercise Point of Contact (e.g., exercise director or exercise sponsor)] |

**For more information about the exercise, please contact:**

Food Defense Assessment Staff

Office of Data Integration and Food Protection  
Food Safety and Inspection Service

U.S. Department of Agriculture

Phone: 202.690.6486  
**E-mail:** [**fooddefense@fsis.usda.gov**](mailto:fooddefense@fsis.usda.gov)

FSIS welcomes your feedback on this exercise. To provide feedback, please go to the FD-PREP website: <https://www.fsis.usda.gov/wps/portal/fsis/topics/food-defense-defense-and-emergency-response/tools-resources-training/fd-prep> and scroll down to “Provide Feedback on FD-PREP”.

Or write to [**fooddefense@fsis.usda.gov**](mailto:fooddefense@fsis.usda.gov)

# General Information

## Exercise Objectives and Core Capabilities

The objectives in Table 1 describe the expected outcomes for the exercise. The objectives are linked to Core Capabilities. Core Capabilities are distinct critical elements necessary to achieve the specific missions. The capabilities listed here are from the list in the National Preparedness Goal by the U.S. Department of Homeland Security.

The exercise planning team chooses the objectives and aligned Core Capabilities for the exercise. For example, you might choose the “Cyber security” and “Access control and identity verification” capabilities for an exercise with the “Test your food defense practices” objective.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Core Capability | Planning | Operational communications | Situational assessment | Public information and warning | Operational coordination | Intelligence and information sharing | Screening, search and detection | Access control and identity verification | Physical protective measures | Cyber security | Risk management for protection programs and activities | Supply chain integrity and security | Long-term vulnerability reduction |
| Objective | | | | | | | | | | | | | |
| Test your food defense plan |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Test your food defense practices |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Test your recall plan |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Test your response and recovery plans |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Test your cyber security procedures |  |  |  |  |  |  |  |  |  |  |  |  |  |

Table 1. Exercise Objectives and Associated Core Capabilities

# Participant Roles and Responsibilities

The term *participant* includes 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.
* **Controllers and Facilitators.** Controllers plan and manage exercise play. They set up and operate the exercise site. They also act in the roles of organizations or individuals that are not playing in the exercise. Facilitators direct the pace of the exercise. They provide key data to players and may prompt or initiate certain player actions to ensure exercise continuity. They also issue exercise materials to players and monitor the exercise timeline. They supervise the safety of all participants. Depending on the size of the exercise, these two roles may be handled by the same person.
* **Evaluators.** Evaluators assess and provide feedback on a specific area of the exercise. Evaluators observe and document performance against capability targets.
* **Observers.** Observers visit or view selected segments of the exercise. Observers do not play in the exercise, nor do they perform any control or evaluation functions. Observers view the exercise from a designated observation area and must remain within the observation area during the exercise.
* **Scribe**. The scribe takes notes during the conduct of the exercise using the online course, or enters responses into the text boxes on interactive PowerPoint presentations.

## Exercise Structure

This exercise is designed to be an interactive, facilitated, tabletop exercise. You will be challenged with an incident, which assumes your current state of readiness. Through the exercise and discussion questions, you may learn some things that will help you improve how prepared you are in the future.

Players can participate in one or more of the following scenarios:

* Scenario 1: Settling the Score
* Scenario 2: Virtual Outrage
* Scenario 3: Smooth Operator
* Scenario 4: Road Rage

The structure of each exercise is :

* **Pre-incident information**: There will be a brief introduction describing a fictitious incident.
* **Incident response to selected scenario**: New information (called “injects”) is given as the incident unfolds. Participants review the situation and have group discussions of important issues. Participants are encouraged to ask questions and learn from one another. The scenarios have been simplified to present the information in an effective way. The intent is to spark discussion of best practices for response.
* **Post-Exercise Debriefing or Hot Wash**: At the conclusion of exercise play, facilitators lead a Hot Wash for players to discuss strengths and areas for improvement.
* **After Action Report and Improvement Planning**: Controllers, facilitators, and exercise leaders hold an After Action Meeting (AAM). The purpose of the AAM is to debrief the exercise and to draft an After Action Report and Improvement Plan to fix weaknesses revealed by the exercise.

## Exercise Guidelines

* This exercise setting will be open, low-stress, and no-fault. Different opinions are expected. Disagreements might even occur.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you might use only existing assets). Draw on your experiences to inform responses.
* Decisions made during the exercise might not reflect your organization’s stance on the issues at hand. This exercise is a chance to explore several possible solutions.

Suggestions that could improve prevention, protection, mitigation, response, and recovery efforts are very important. They should be the focus of the discussion. Don’t focus on figuring out the causes of the situations presented in the exercise or get too caught up in small details.

## Exercise Assumptions and Artificialities

Some assumptions might be necessary to complete play in the time given. Exercise participants should play along with the scenario. Do not allow unrealistic features to negatively impact participation. During this exercise, the following premises apply:

* The exercise occurs in a no-fault learning environment. Capabilities, plans, systems, and processes will be evaluated.
* The exercise scenario is plausible, and events occur as they are presented.
* All players receive information at the same time.
* The exercise should reflect current FSIS rules, regulations, policies, and procedures.

## Exercise Planning

The exercise controller and facilitators will hold a planning meeting in advance of the exercise to decide on the objectives and aligned Core Capabilities to be tested. The team will also select exercise participants with the goal of making the discussion and post-exercise documents as useful as possible.

## Exercise Logistics

### Time Requirement

Each scenario is expected to be completed in 60-90 minutes. Allow additional time on the day of the exercise to print out player handouts (e.g., Situation Manual and Participant Feedback Forms), set up seating suitable for a discussion, set up audiovisual equipment, and to brief players and observers.

### Security

If security measures are required to enter the location(s) for the exercise, the sponsor organization should arrange access. Players should report any unauthorized persons.

### Observer Coordination

Organizations with observers attending the event should coordinate with the sponsor organization for access to the exercise site. Observers are escorted to designated areas. They should be accompanied by an exercise controller at all times. Sponsor organization representatives and/or the observer controller may be present to explain exercise conduct and answer questions. Exercise participants should be told observers are present.

# 

# Participant Information and Guidance

## Exercise Rules

The following general rules apply to exercise play:

* If a real-world emergency occurs while the exercise is being conducted, the real emergency takes priority over exercise actions.
* Exercise players will follow real-world emergency procedures, unless told otherwise by the facilitators.
* Begin and end any requests for information outside the exercise setting with “Exercise, Exercise, Exercise” to avoid confusion.

## Player Instructions

Follow the guidelines below to ensure a safe and useful exercise.

### Before the Exercise

* Review appropriate organizational plans, procedures, and exercise support documents.
* Sign in when you arrive.
* Be at the appropriate site at least 30 minutes before the exercise starts. Wear the appropriate uniform and/or identification item(s).
* If you learn of the scenario before the exercise, inform a facilitator so that action can be taken to ensure a valid evaluation.

### During the Exercise

* Respond to exercise events and information as if the situation were real, unless told otherwise by a facilitator.
* Facilitators will give you only information they are directed to provide. You are expected to obtain other needed information through existing channels.
* Ask questions if you are unsure about anything in the exercise scenario.
* Parts of the scenario might seem unlikely. Recognize that the exercise has objectives to satisfy and might require some unrealistic features. Every effort has been made to balance realism with safety. Attention was given to creating an effective learning and evaluation environment.

### After the Exercise

* Participate in the Post Exercise Debriefing or Hot Wash at your venue with facilitators and controllers.
* Complete the participant feedback form. This form allows you to comment freely on response activities and exercise effectiveness. Provide the completed form to a facilitator.

Provide any notes or materials from the exercise to your facilitator for review and inclusion in the After Action Report.

# Facilitator Information and Guidance

## Exercise Control Overview

Exercise control maintains exercise scope, pace, and integrity during exercise conduct. It ensures that exercise play assesses objectives in a coordinated fashion at all levels throughout the whole exercise.

## Facilitator Instructions

### Before the Exercise

* Review appropriate emergency plans, procedures, and protocols.
* Review appropriate exercise package materials, including the objectives, scenario, injects, and facilitator instructions.
* Attend required briefings.
* Be at the appropriate location at least 30 minutes before the exercise starts.
* Obtain, locate, and test necessary communications equipment.
* Prepare the meeting room and materials, then introduce and lead the exercise.

### During the Exercise

* Review participant roles at the beginning of the exercise.
* Encourage the group to interact as they would in the “real world.” Encourage the participants to share their experiences and ideas so that they can learn from one another.
* Identify participants who have relevant and recent experience with scenarios such as this. Encourage them to share with less experienced participants.
* Ensure that players have all the information they need to play. Facilitators should observe and record any parts of the exercise that interfere with realism.
* There are not necessarily right or wrong answers. Participation and discussion is what is important. You will have the chance at the end of the exercise to determine what is right for your establishment.
* Do not prompt players regarding what a specific response should be, unless an inject directs you to do so. Clarify information but do not provide coaching.
* Address participant concerns during the exercise
* Wear facilitator identification items (e.g., badge).
* Ensure that all observers stay out of the exercise activity area.

### After the Exercise

* Distribute copies of Participant Feedback Forms and relevant documentation.
* All facilitators are expected to conduct a Post Exercise Debriefing, or Hot Wash, at their venue and take notes on findings identified by exercise players. Before the Hot Wash, do not discuss specific issues or problems with exercise players.
* At the end of the exercise, facilitators should sum up their notes from the exercise and Hot Wash, and have the summary ready for evaluation.

|  |
| --- |
| **Controller/ Facilitator Responsibilities** |
| * Oversees all exercise functions * Oversees and remains in contact with other controllers and facilitators * Oversees setup and takedown of exercise * Monitors exercise progress * Observes and records any exercise parts that interfere with exercise realism * Coordinates decisions regarding significant changes to the scenario * Issues exercise materials to players * Provides input to players (i.e., injects) * Serves as safety officer for his or her site |

Table 3. Controller/Facilitator Responsibilities. More than one set of responsibilities may be discharged by one person.

# Post-Exercise and Evaluation Activities

### Post-Exercise Debriefing or Hot Wash

When the exercise ends, controllers or facilitators lead a Hot Wash to allow players to discuss strengths and areas for improvement. It also allows evaluators to seek clarification regarding player actions and decisionmaking. All participants may attend. However, observers are not encouraged to attend the meeting, since the information generated will be confidential to the establishment. The Hot Wash should not exceed 30 minutes.

### Participant Feedback Forms

Participant Feedback Forms provide players with the opportunity to comment freely on exercise activities and exercise design. Participant Feedback Forms should be collected at the conclusion of the Hot Wash.

## Evaluation

### After Action Meeting (AAM)

The After Action Meeting (AAM) is a meeting held among decisionmakers from the exercising organizations, the facilitator, and the exercise planning team. The AAM is designed to debrief the exercise and to review and refine the draft AAR and Improvement Plan (IP). The AAM should be interactive and provide attendees the opportunity to talk about and confirm the observations and corrective actions in the draft AAR/IP.

### After Action Report (AAR)

The AAR summarizes key information related to evaluation. The AAR primarily focuses on the analysis of Core Capabilities, how the objectives were achieved, strengths, and areas for improvement. AARs also include basic exercise information. This includes the exercise name, type of exercise, dates, location, participating organizations, mission area(s), specific threat or hazard, a brief scenario description, and the name of the exercise sponsor and Point of Contact (POC).

## Improvement Planning

Improvement planning is the process of resolving the observations recorded in the AAR through development of the Improvement Plan (IP). The IP identifies concrete corrective actions, which are prioritized and tracked as a part of a continuous corrective action program. The IP assigns the corrective actions to responsible parties and sets target dates for their completion. It is created by officials from the organizations participating in the exercise. It is discussed and validated during the AAM.

# Exercise Evaluation Guidance

## Exercise Evaluation Overview

Exercise evaluation assesses an organization’s capabilities to accomplish a mission, function, or objective. Evaluation provides an opportunity to assess performance of critical tasks to capability target levels. Evaluation is accomplished by:

* Observing the event and collecting supporting data;
* Analyzing collected data to identify strengths and areas for improvement; and
* Reporting exercise outcomes in the AAR.

## Evaluation Documentation

### After Action Report/Improvement Plan (AAR/IP)

The main focus of the AAR is the analysis of Core Capabilities. For each Core Capability exercised, the AAR includes strengths and areas for improvement.

Organization leaders confirm observations identified in the draft AAR and determine which areas for improvement require further action. As part of the improvement planning process, leaders identify corrective actions to resolve areas for improvement and determine the appropriate entity responsible for those actions. Corrective actions are consolidated in the IP. The IP is included as an appendix to the AAR.

### Exercise Evaluation

#### Terminology

* **Core Capabilities:** The distinct critical elements necessary to achieve a specific mission area (e.g., prevention). To assess both capacity and gaps, each Core Capability includes capability targets.
* **Capability target(s):** The performance thresholds for each Core Capability. They state the exact *amount* of capability that players aim to achieve. Capability targets are typically written as quantitative or qualitative statements. For example, a capability target might state, “*Within 4 hours of the incident….”*
* **Performance ratings:** The summary description of performance against target levels. Performance ratings include both Target Ratings and Core Capability Ratings. Target Ratings describe how exercise participants performed relative to each capability target. Core Capability Ratings describe overall performance relative to the entire Core Capability.

#### Documenting Observations

Observation notes should include *if* and *how* quantitative or qualitative targets were met. Notes on that target should include the actual time required for exercise players to complete the critical tasks. Additionally, observations should include:

* How the target was or was not met;
* Appropriate decisions made and information gathered to make decisions;
* Requests made and how requests were handled;
* Resources utilized;
* Plans, policies, procedures, or legislative authorities used or implemented; and
* Any other factors that contributed to the results.

Evaluators should also note if an obvious reason resulted in players not meeting a capability target or critical task. During the after action and improvement planning processes, organization leaders will review and confirm observations documented in the AAR. They will also determine areas for improvement requiring further action.

*Note:* Observation notes for discussion based exercises will focus on *discussion* of how critical tasks would be completed, rather than actual actions taken.

#### Assigning Ratings

Based on their observations, evaluators assign a rating for each Core Capability exercised*.* Evaluators then consider all ratings for the Core Capability and assign an overall Core Capability rating. The rating scale includes four ratings:

**Performed Without Challenges (P):** The targets and critical tasks associated with the Core Capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

**Performed With Some Challenges (S):** The targets and critical tasks associated with the Core Capability were completed in a manner that achieved the objective(s) and did not negatively impact the performance of other activities. Performance of this activity did not contribute to additional health and/or safety risks for the public or for emergency workers, and it was conducted in accordance with applicable plans, policies, procedures, regulations, and laws. However, opportunities to enhance effectiveness and/or efficiency were identified.

**Performed With Major Challenges (M):**  The targets and critical tasks associated with the Core Capability were completed in a manner that achieved the objective(s), but some or all of the following were observed: demonstrated performance had a negative impact on the performance of other activities; contributed to additional health and/or safety risks for the public or for emergency workers; and/or was not conducted in accordance with applicable plans, policies, procedures, regulations, and laws.

**Unable To Be Performed (U):** The targets and critical tasks associated with the Core Capability were not performed in a manner that achieved the objective(s).

### Placement and Monitoring

Evaluators should be located so they can observe player actions and hear conversations without interfering. If players are broken out into multiple groups in larger exercises, separate evaluators would be required to observe each group.

# Exercise Presentation Information

FSIS offers two options for accessing and presenting FD-PREP: Online course and downloadable PowerPoint presentations.

## Online Course

* A version of FD-PREP can be accessed on the FSIS website as an online course without the need to download the scenarios.
* A key benefit of this option is that it is accessible to people with disabilities while including advanced features (e.g., interactive buttons, media elements, menus).
  + The accessibility and usability features are explained in more detail here: <http://www7.courseavenue.com/section508features.aspx>
* Users choosing this option should rely on the scribe in their group to take notes in a separate document during the exercise (there are no built-in text boxes onscreen).

### Online Course Navigation

The user navigates through the course using four key buttons (example below):

1. **Next:** Goes to the next page in the course.
2. **Back:** Goes back one page in the course.
3. **Help:** Opens a new window that provides extra information, such as course navigation, keyboard shortcuts, and accessibility usage hints.
4. **Menu:** Brings the user to the Table of Contents.
   * *Note*: In a web-only course, users cannot save their spot in the course if they don’t finish in one sitting. So, if needed, they should use the menu to get back to where they left off.



4

3

2

1

More features:

* **Progress Bar:** The built-in progress bar shows which page the user is on.
* **Exit Course:** Users can exit out of the course at any time by closing the webpage or clicking the X (exit button) in the top right corner of the course.
* **Other Navigation Options:** There are times users might be told to choose a button onscreen to go to a different page, instead of clicking Next or Back. In these cases, there will be onscreen instructions.
* **Opening Audio Transcripts:** Users can open and close the Audio Transcript Window using the gray Audio Script Button. Screenshot of a gray button with a speech bubble on it. This button opens and closes the audio transcript window in the course.

The Audio Script Button appears on any pages with an available transcript.

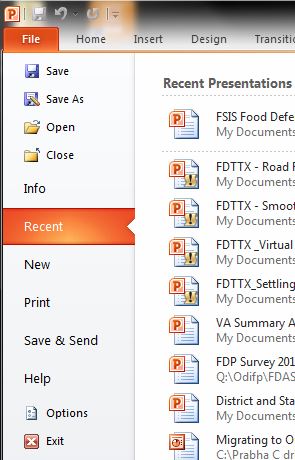
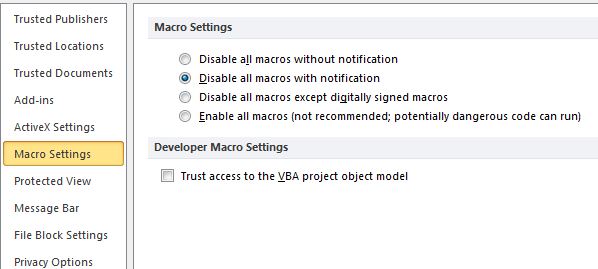
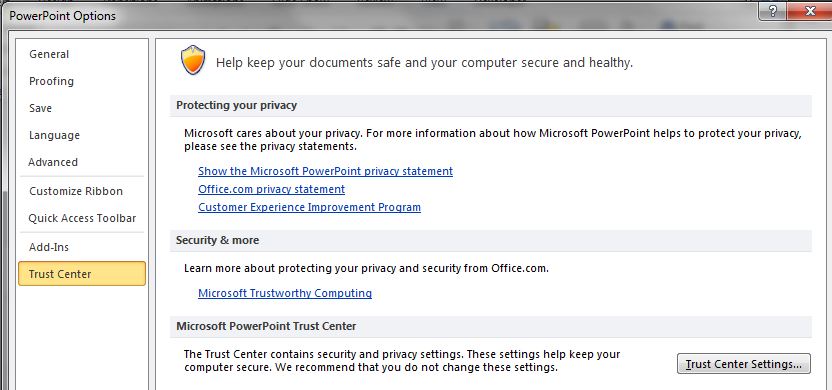
## PowerPoint

* This exercise can also be accessed as four separate downloadable PowerPoint files. This version is more suitable for users who might not have Internet access at the exercise site. The PowerPoint files can be downloaded and presented later at your convenience.
* An advantage of the PowerPoint version is that once downloaded, the presentation may be customized to your particular situation. For example, where the original presentation refers to “a product that you produce,” that phrase could be replaced with the name of one of your products.
* In this version, text boxes are available on the slides with questions. These text boxes can be used to record and save answers. This means that the scribe will not be required to take notes by hand. Also, all players can see the answers as they are being typed in, which might encourage additional thinking and more suggestions.

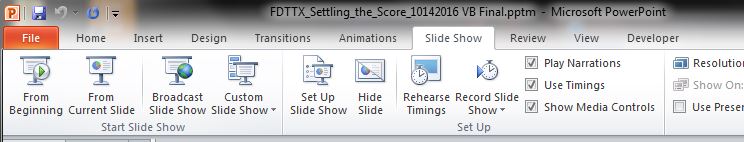
### PowerPoint Navigation

*Note: These instructions apply to PowerPoint 2010. If you are using a different version, the steps might vary slightly.*

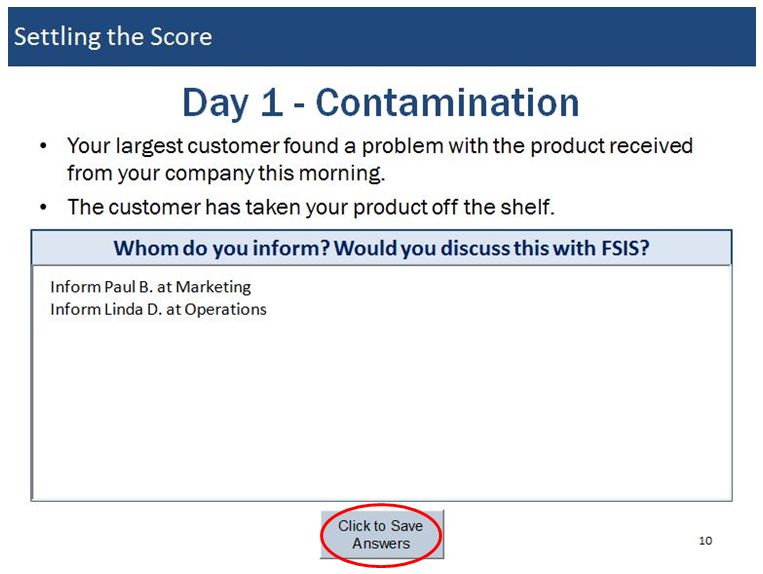
* Before starting the presentation, please enable macros in PowerPoint. This will allow you to use the full functionality of the presentation. In PowerPoint, click the **File** menu at top left, and then choose **Options** from the menu at left. In the dialogue box that opens, choose **Trust Center** from the menu at left, and then click **Trust Center Settings**. In the next dialogue box, click **Disable all macros with notification**. Click **OK**.



* To view the presentation, open the file and click **Slide Show** from the top menu bar, then click on **From Beginning** at far left. Clicking anywhere on the slide in Slide Show mode will advance the presentation to the next slide. **Page Up/ Page Down** buttons can be used to navigate forward and backward in the presentation.



* As you advance through the presentation, enter answers to questions in the text boxes. Clicking the **Click to Save Answers** button will save answers.



* At the end of the presentation, all answers saved from text boxes will be automatically combined and saved into a Word document. This document will be created in the same directory as the PowerPoint presentation and will be named “Scenario Name Exercise\_yyyy-mm-dd.doc”. For example, if you conducted the Settling the Score exercise on November 3, 2016, the resulting file will be named “Settling the Score Exercise\_2016-11-03.doc”. This document can be used as a starting point to build the AAR/IP.

If you conduct the exercise more than once on the same day, then the answers from the second run will be added to the end of the original document. Alternatively, you may rename the output file from the first run, and the second run will produce a new document as described above.

# Exercise Scenarios

## Scenario 1: Settling the Score (Disgruntled Employee scenario)

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

The events described occur at an FSIS regulated establishment producing meat, poultry, processed egg products, or fish of the order Siluriformes. Parties involved are establishment personnel, customers, FSIS inspectors, law enforcement. The establishment’s product might have been adulterated by a disgruntled former employee. Management has to work together to deal with law enforcement and media, minimize public health effects, and ensure business continuity.

## Key Issues and Supplemental Questions

These additional notes and questions are meant to be used along with the scenario presentation and prompt further discussion. The day number in the table below corresponds to the day in the scenario. Use these to encourage dialogue and sharing, but try not to guide the discussion in a particular direction (PP: PowerPoint, OC: Online Course).

| Unit | Key Issues | Questions |
| --- | --- | --- |
| Welcome/ Intro  PP Slides 1-8  OC Pages 1-8 | * Introduction * Objectives * Participant Roles * Exercise Structure |  |
| Day 1  PP Slides 9-12  OC Pages 9-12 | * Threat Notification * Standard Operating Procedures * Traceability | * Do you have records of the lot numbers delivered to each customer? * What is your plan for responding to customer complaints? * Who will be informed about the customer complaint? |
| Day 2  PP Slides 13-14 OC Pages 13-14 | * Employee Impact * Media Coverage * Investigation | * How would you operate with fewer employees than usual? Can you hire additional temporary employees? * Do you have a designated emergency response team? Who is on this team? |
| Day 5  PP Slides 15-19 OC Pages 15-19 | * Public Health Impact * Communications Plans * Recall Plans | * What communication activities, internal or external, should be initiated? * Who will deal with public health officials and law enforcement agencies? * How would you limit access/exposure to the suspect product and processing facilities? * Do you have a plan for recalling product if required? * What recordkeeping processes do you have in place to ensure that you would be able to properly track products? * Should you contact your company’s lawyers? |
| Day 15  PP Slides 20-22 OC Pages 20-22 | * Law Enforcement * Continuity of Operations | * Food safety incidents are not usually treated as a crime scene, but food defense incidents are likely to be. This brings in additional responders to your establishment, including law enforcement. * Does your liability insurance cover this incident? * Who is responsible for implementing your recall plan? * Do you have contact information for all your customers? |
| Day 16  PP Slides 23-24 OC Pages 23-24 | * Media Coverage * Communication Plans | * Do you have a designated spokesperson? * Who is responsible for communicating with employees, customers, suppliers, media? * How will you communicate with these different groups? * Who creates, reviews, and approves the messages? * Who decides what information should not be released to protect the investigation? |
| Day 17  PP Slides 25-26 OC Pages 25-26 | * Business Impact * Business Continuity * Product Recall and Recovery | * Do you have plans for dealing with a plant closure? * Do you have business interruption insurance that will cover extended closure? * Do you have a plan for storing or destroying recalled product? * How would you manage consumer questions and fear during the recall of your product due to intentional contamination? |
| Day 21  PP Slides 27-31 OC Pages 27-31 | * Security Measures * Background Checks * Suspicious Behavior | * Some people think of outside terrorist groups when they think of intentional contamination. Disgruntled employees may be the more likely threat, though often their capabilities are less than what a terrorist organization is capable of. * Are there standard security procedures when an employee leaves the company? * When an employee leaves, is that person’s access badge taken? * If doors have access codes, are they changed when an employee leaves or is terminated? * Are other employees made aware when someone is terminated? * Do you train employees to watch for suspicious behavior? |
| Wrap Up  PP Slides 32-36 OC Pages 32-36 | * Food Defense Plans * Written Recall Procedures | * What went right, and what can you improve on, at each stage of the incident response? * Can you easily access contact information for all your customers, suppliers, employees, lawyers, insurers, local law enforcement authorities, and FSIS? Can you access it even if your facility computers fail? * What changes are needed to physical and equipment security or management processes? * What training is needed for employees and management? |

##### **Notes**

A specific chemical is not named in this exercise. Try not to have the group get “hung up” on the contaminant or the chance that a certain contaminant was used.

In a food defense context, there are two special factors about contaminants that often don’t apply in food safety scenarios:

The contaminant might not be one you know or regularly test for.

The contaminant might survive cooking or other processing steps.

## Scenario 2: Virtual Outrage (Cyber Threat scenario)

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

The events described occur at an FSIS-regulated establishment producing meat, poultry, processed egg products, or fish of the order Siluriformes. Parties involved are establishment personnel, customers, FSIS inspectors, and law enforcement. The establishment’s automated control systems are locked by a ransomware attack. Management has to work together to deal with law enforcement and media, minimize public health effects, and ensure business continuity.

## Key Issues and Supplemental Questions

These additional notes and questions are meant to be used along with the scenario presentation and prompt further discussion. The day number in the table below corresponds to the day in the scenario. Use these to encourage dialogue and sharing, but try not to guide the discussion in a particular direction (PP: PowerPoint, OC: Online Course).

| Unit | Key Issues | Questions |
| --- | --- | --- |
| Welcome/Intro  PP Slides 1-8 OC Pages 1-8 | * Introduction * Objectives * Participant Roles * Exercise Structure |  |
| Day 1  PP Slides 9-13 OC Pages 37-42 | * Information Security Awareness * Standard Operating Procedures * Cyber Risk Assessment | * Are your employees aware that cyber threats can have severe consequences for your business? * Ransomware is not the only threat to your IT infrastructure. What other threats do you know of? |
| Day 4  PP Slides 14-18 OC Pages 43-47 | * Training * Device and Network Access Control * Cyber Security Monitoring Methods * Information Dissemination | * How often do employees receive training on IT security? * How can you control access to the network and other IT infrastructure? * How can you prevent unauthorized software from being introduced to the system? What security measures can be put in place? How will employees be trained? * Are employees aware of “phishing” attacks? What kind of information might the attackers ask for? * What do employees know about identity theft, and how to protect themselves? |
| Day 7  PP Slides 19-22 OC Pages 48-51 | * Data Security and Back Up | * What types of tools and processes are available to detect and contain cyber attacks? How do these tools help with identification and resolution of the cyber attack? * Are they automated services that provide alerts? Or do they require manual engagement? * What external providers could you tap to analyze your network for intrusions and other problems? |
| Day 9  PP Slides 23-26 OC Pages 52-55 | * Communication Plan * Incident Escalation | * Whose responsibility is it to check for equipment performance issues such as temperature fluctuations in freezers, or accuracy in labels? To whom should they communicate any issues? * What happens after an issue like this is detected? Should other systems be checked immediately (e.g., IT system back up, alarm system, video or other monitoring system, processing equipment systems)? * How soon should the issue be reported to top management? |
| Day 9  PP Slides 27-35 OC Pages 56-63 | * Business Impact * Business Continuity * Law Enforcement * Third-Party Security Providers | * Do you have business interruption insurance that will cover extended closure? * Do you have a plan for dealing with plant closure? * Would you consult with law enforcement at this time? Who will deal with law enforcement agencies? * Does your liability insurance cover this incident? When would you report this to your insurer? Should you contact your company’s lawyers? * How will you trace and recall if your computers are malfunctioning? * What outside providers could you hire to help you in this situation? |
| Wrap Up  PP Slides 36-40 OC Pages 64-69 | * Food Defense Plans * Steps to Avoid Cyber Incidents | * What went right, and what can you improve on, at each stage of the incident response? * Can you easily access contact information for all your customers, suppliers, employees, lawyers, insurers, local law enforcement authorities, and FSIS? Can you access it even if your facility computers fail? * What changes are needed to physical and equipment security or management processes? * What training is needed for employees and management? |

## Scenario 3: Smooth Operator (Insider Threat scenario)

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

The events described occur at an FSIS-regulated establishment producing meat, poultry, processed egg products, or fish of the order Siluriformes. Parties involved are establishment personnel, customers, FSIS inspectors, and law enforcement. An activist group has spread a video accusing the establishment of violating food safety regulations. Management has to work together to deal with law enforcement and media, minimize public health effects, and ensure business continuity.

## Key Issues and Supplemental Questions

These additional notes and questions are meant to be used along with the scenario presentation and prompt further discussion. The day number in the table below corresponds to the day in the scenario. Use these to encourage dialogue and sharing, but try not to guide the discussion in a particular direction (PP: PowerPoint, OC: Online Course).

| Unit | Key Issues | Questions |
| --- | --- | --- |
| Welcome/Intro  PP Slides 1-8  OC Pages 1-8 | * Introduction * Objectives * Participant Roles * Exercise Structure |  |
| Day 1  PP Slides 9-15  OC Pages 70-77 | * Standard Operating Procedures * Communication Plan * Background checks | * Violations claimed by the activists could include humane-handling violations, sanitation violations, etc. * Do you have a designated person who will talk to media and law enforcement authorities? Who creates, reviews, and approves the messages? * Who decides what information should not be released to protect the investigation? * Other than background checks, are there any security measures that could be used to vet employees and contractors? |
| Day 2  PP Slides 16-19  OC Pages 78-81 | * Monitoring * Recordkeeping | * Do you have video surveillance of your processing operations? * Do you provide training to employees on following all regulations? Do you keep records of these trainings? |
| Day 3  PP Slides 20-26  OC Pages 82-88 | * Inventory Storage * Business Impacts * Access Control | * How would you manage consumer inquiries and fear during this time? * Do you have plans for dealing with a plant closure? * Do you have business interruption insurance that will cover extended closure? * Have you talked to your establishment’s lawyers? * Can you use badges or locks so that only employees needing to be in a particular work area can enter it? |
| Day 4  PP Slides 27-30  OC Pages 89-92 | * Dry Ingredients * Quality Control * Trace-Forward Procedures * Recall Procedures | * Can ingredient areas be locked? * What receiving procedures are in place to ensure ingredient quality? * Do you have a plan for recalling product if required? * What recordkeeping processes do you have in place to ensure that you would be able to appropriately track products? |
| Day 9  PP Slides 31-33  OC Pages 93-95 | * Reporting Mechanisms * Workplace Culture | * Can you provide an anonymous suggestion box where employees can report incidents and avoid backlash? * Do you provide training to supervisors on how to handle reports of suspicious activity? |
| Day 12  PP Slides 33-36  OC Pages 96-98 | * Media Coverage * Communication Plans | * Do you have a designated spokesperson? * Do you have a plan for communicating with law enforcement authorities, employees, customers, suppliers, and media? * What measures do you have in place to protect your facility, your employees, and your product? |
| Day 14  PP Slides 37-39  OC Pages 99-101 | * Employee Training * Insider Threat Awareness | * Do employees know what the term “insider threat” means? * Do you train employees to watch for suspicious behavior? * Are other employees made aware when someone is terminated? Are they told why the person was terminated? |
| Wrap Up  PP Slides 40-44  OC Pages 102-106 | * Food Defense Plans * Preparedness Against Insider Threats | * What went right, and what can you improve on, at each stage of the incident response? * Can you easily access contact information for all your customers, suppliers, employees, lawyers, insurers, local law enforcement authorities, and FSIS? Can you access it even if your facility computers fail? * What changes are needed to physical and equipment security or management processes? * What training is needed for employees and management? |

## Scenario 4: Road Rage (Transportation Threat scenario)

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

The events described occur at an FSIS-regulated establishment producing meat, poultry, processed egg products, or fish of the order Siluriformes. Parties involved are establishment personnel, customers, FSIS inspectors, and law enforcement. The establishment’s product is stolen by an imposter transport contractor. Management has to work together to deal with law enforcement and media, minimize public health effects, and ensure business continuity.

## Key Issues and Supplemental Questions

These additional notes and questions are meant to be used along with the scenario presentation and prompt further discussion. The day number in the table below corresponds to the day in the scenario. Use these to encourage dialogue and sharing, but try not to guide the discussion in a particular direction (PP: PowerPoint, OC: Online Course).

| Unit | Key Issues | Questions |
| --- | --- | --- |
| Welcome/Intro  PP Slides 1-8  OC Pages 1-8 | * Introduction * Objectives * Participant Roles * Exercise Structure |  |
| Day 1 – 9.00 AM  PP Slides 9-17  OC Pages 107-116 | * Access Control * Background Checks * Standard Procedures | * Do you have locks on the doors to your processing areas? If you have badge access, how often is the access log reviewed? * Do you post “Employees Only” signs or other similar signage? * Do you perform background checks for employees and others who regularly enter your facility? * Are all your employees aware of standard procedures in the establishment? How can you ensure that the procedures are followed? |
| Day 1 – 9.20 AM  PP Slides 18-20  OC Pages 117-119 | * Employee Training * Food Defense * Ingredient Storage | * Are other employees made aware when a contractor or other partner has changed? * What training do employees receive on interactions with contractors and other partners? * Can you use badges or locks so that only employees needing to be in a particular work area can enter it? * Have you considered the possibility that someone could intentionally adulterate your product? What measures are in place to prevent such adulteration? |
| Day 1 – 10.00 AM  PP Slides 20-22  OC Pages 120-121 | * Sealing Protocols * Packaging | * Are outgoing shipments sealed, and are seal numbers noted in a log? * Do you inspect seals on incoming shipments? |
| Day 2 – 9.00 AM  PP Slides 23-25 OC Pages 122-124 | * Business Impacts * Law Enforcement | * Do you have a designated person who will talk to FSIS, law enforcement officials, media, or other outside parties? |
| Day 2 – 1.00 PM  PP Slides 26-27  OC Pages 125-126 | * Product Testing * Product Disposal | * Since the truck crossed State lines, the Federal Bureau of Investigation (FBI) will be involved. Do you know how to contact your local FBI field office? * Would you be able to tell if your packaging has been broken and then resealed? * How would you dispose of a large amount of product, if necessary? |
| Day 2 – 4.00 PM  PP Slides 28-30  OC Pages 127-129 | * Ingredient Testing * Recall Plans * Business Closure Plans | * What types of agents would you consider testing the dry ingredients for? * Would it be more economical to throw away all potentially adulterated ingredients and buy new ones? |
| Day 14  PP Slides 31-33  OC Pages 130-132 | * Employee Training * Insider Threat Awareness | * Do employees receive food defense training? How often does training occur? * Do employees know what the term “insider threat” means? * Do you train employees to watch for suspicious behavior? * What should employees do if they observe suspicious behavior? |
| Wrap Up  PP Slides 35-39  OC Pages 133-137 | * Food Defense Plans * Preparedness Against Insider Threats | * What went right, and what can you improve on, at each stage of the incident response? * Can you easily access contact information for all your customers, suppliers, employees, lawyers, insurers, local law enforcement authorities, and FSIS? Can you access it even if your facility computers fail? * What changes are needed to physical and equipment security or management processes? * What training is needed for employees and management? |

# Appendix A: Exercise Schedule

**[Note:** Because this information is updated throughout the exercise planning process, appendixes may be developed as stand-alone documents rather than part of the C/F Handbook.]

| **Time** | **Personnel** | **Activity** | **Location** |
| --- | --- | --- | --- |
| **[Date]** | | | |
| [Time] | Controllers and exercise staff | Check-in for final instructions and communications check | [Location] |
| [Time] | Media | Media Briefing | [Location] |
| [Time] | Controllers and evaluators | Controllers and facilitators in starting positions | [Location] |
| [Time] | All | Controllers provide player briefs | [Location] |
| [Time] | All | Exercise starts | [Location] |
| [Time] | All | Exercise ends | [Location] |
| Immediately Following the Exercise | All | Venue Hot Washes/turn in all Participant Feedback Forms | [Location] |
| **[Date]** | | | |
| [Time] | Controllers, evaluators, | Controller and Facilitator After Action Review | [Location] |

# Appendix B: Exercise Participants

|  |
| --- |
| **Participants** |
| Establishment Personnel |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Observers |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
| Others |
|  |
|  |
|  |
|  |

# Appendix C: Acronyms

|  |  |
| --- | --- |
| Acronym | Term |
| AAM | After Action Meeting |
| AAR | After Action Report |
| FBI | Federal Bureau of Investigation |
| FSIS | Food Safety and Inspection Service |
| IP | Improvement Plan |
| USDA | United States Department of Agriculture |
| HSEEP | Homeland Security Exercise and Evaluation Program |
| C/F | Controller/Facilitator |
| POC | Point of Contact |
| PP | PowerPoint |
| OC | Online Course |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |