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



**United States Department of Agriculture**

Exercise Guide

[Date]

This Handbook describes the roles and responsibilities of exercise leaders and participants. It also describes the procedures they should follow. Leaders may choose to provide all or parts of it to participants.

Please note that all the information in this guide may not apply to all exercises that may be run using this toolkit. Exercise leaders may adapt the instructions to their situation, if needed.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Food Defense Preparedness and Recall Exercise Package (FD-PREP) |
| **Establishment Name** | [Insert Establishment Name] |
| **Exercise Dates** | [Indicate the date of the exercise] |
| **Scope** | This is a tabletop exercise planned for 60-90 minutes. It is for FSIS-regulated establishments or others who wish to test food defense plans or food defense practices. |
| **Mission Area(s)** | Prevention, Protection, Mitigation, Response, Recovery |
| **Core Capabilities**  (As defined by the U.S. Department of Homeland Security) | **Choose the Core Capabilities you want to test:**  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  Cybersecurity  Risk management for protection programs and activities  Supply-chain integrity and security  Long-term vulnerability reduction |
| **Exercise Objectives** | Test your establishment’s food defense plan  Test food defense practices at your establishment  Test your establishment’s recall plan  Test your establishment’s response and recovery plans  Test the cybersecurity practices at your establishment |
| **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. |
| **Point of Contact** | [Insert the name, title, address, phone number, and email address of the primary exercise Point Of Contact (e.g., exercise leader or facilitator)] |

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

The objectives in Table 1 describe the expected outcomes for the exercise. The exercise leaders choose the objectives.

|  |
| --- |
| **Exercise Objectives** |
| * Test your establishment’s food defense plan |
| * Test food defense practices at your establishment |
| * Test your establishment’s recall plan |
| * Test your establishment’s response and recovery plans |
| * Test the cybersecurity practices at your establishment |

Table 1. Exercise Objectives

## Participant Roles and Responsibilities

The term *participant* includes many groups of people, not just those playing in the exercise. Each exercise role is described in detail below:

* **Players.** Players have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or take actions in response to the scenario.
* **Leaders 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.
* **Observers.** Observers visit or view selected parts of the exercise. Observers do not play in the exercise. They also do not control or evaluate anything. 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 exercise using the online interactive format, or enters responses into the text boxes on interactive PowerPoint presentations.

## Exercise Structure

This exercise is an interactive, facilitated tabletop exercise. You will be challenged with an incident, which you will deal with at 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.

You may exercise one or more of the scenarios on a given day:

* 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 is 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 goal is to spark discussion of best practices for response.
* **Post-Exercise Debriefing or Hot Wash**: At the end of exercise play, facilitators lead a Hot Wash for players to discuss strengths and areas for improvement.
* **After Action Report and Improvement Planning**: Decisionmakers, facilitators, and exercise leaders hold an After Action Meeting (AAM). The purpose of the AAM is to debrief the exercise and draft an After Action Report and Improvement Plan to fix weaknesses revealed by the exercise.

## Exercise Guidelines and Assumptions

* This exercise setting will be open, low-stress, and no-fault. Different opinions are expected. Disagreements may even occur.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may use only existing resources). Use your experiences to come up with responses.
* Exercise participants should assume that the scenario is possible and events happen as presented. Participants should play along with the scenario. Do not allow unrealistic parts to negatively impact participation.
* The exercise should reflect current FSIS rules, regulations, policies, and procedures.
* 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 scenarios or get too caught up in small details.

## Exercise Planning

The exercise leaders may hold a planning meeting beforehand to choose the objectives to test. They will also select exercise participants with the goal of making the discussion and post-exercise documents as useful as possible.

## Time Requirement

Each scenario is expected to take 60-90 minutes. Allow extra time on the day of the exercise to print out player handouts and participant feedback forms, set up seating for a discussion, and set up audiovisual equipment. Extra time should also be allowed to brief players and observers and to conduct a post-exercise debriefing session or Hot Wash.

# Participant Information and Guidance

## Exercise Rules

* If a real-world emergency happens during the exercise, the real emergency takes priority over the exercise.
* Exercise players will follow real-world emergency procedures, unless told otherwise by the facilitators.
* If you call for any information from outside the exercise setting, begin and end the request with “Exercise, Exercise, Exercise” to avoid confusion.

## Player Instructions

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

### Before the Exercise

* Review relevant organizational plans, procedures, and exercise support documents.
* Sign in when you arrive.
* Be at the 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, tell a facilitator.

### During the Exercise

* Respond to exercise events and information as if the situation were real, unless told otherwise by a facilitator.
* Facilitators will only give you information they are told 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 may seem unlikely. Recognize that the exercise has objectives to satisfy and may 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 with facilitators.
* Complete the participant feedback form. This form allows you to comment freely on exercise activities and usefulness. Give the completed form to a facilitator.

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

# Facilitator Information and Guidance

## Facilitator Instructions

### Before the Exercise

* Review appropriate emergency plans and procedures.
* Review the exercise package materials (i.e., objectives, scenario, injects, and facilitator instructions).
* Be at the correct location at least 30 minutes before the exercise starts.
* Find and test needed 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 members 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. Facilitators should observe and record any parts of the exercise that make the exercise not seem realistic.
* 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 decide what is right for your establishment.
* Do not tell players what a specific response should be, unless an inject tells you to do so. Clarify information but do not provide coaching.
* Address participant concerns during the exercise

### After the Exercise

* Distribute copies of participant feedback forms and relevant documentation.
* All facilitators conduct a Post Exercise Debriefing, or Hot Wash, and take notes on the exercise players’ findings. Do not discuss specific issues with exercise players before the Hot Wash.
* After the end of the exercise, facilitators should sum up their notes from the exercise and Hot Wash and have the summary ready for After Action Report development.

|  |
| --- |
| **Facilitator Responsibilities** |
| * Oversees all exercise functions * 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 2. Facilitator Responsibilities.

# Post-exercise and Evaluation Activities

### Post-Exercise Debriefing or Hot Wash

After the exercise, controllers or facilitators lead a Hot Wash. The Hot Wash allows players to discuss strengths and areas for improvement. It also allows controllers and facilitators to clarify 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 20 minutes.

### Participant Feedback Forms

Participant feedback forms give players the chance to comment freely on exercise activities and design. Participant feedback forms should be collected at the end of the Hot Wash.

## Evaluation

### After Action Meeting (AAM)

The AAM is a meeting with decisionmakers from the establishment, the facilitator, and the exercise leaders. The AAM is designed to debrief the exercise and to review and improve the draft After Action Report (AAR) and Improvement Plan (IP). The AAM should be interactive and give 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 mainly focuses on analyzing core capabilities, how the objectives were achieved, strengths, and areas for improvement. AARs also include basic exercise information. This includes the exercise name, dates, location, specific threat or hazard, a brief scenario description, and the name of the exercise Point of Contact (POC).

## Improvement Plan (IP)

Improvement planning is the process of using the observations from the AAR to develop an IP with concrete corrective actions. The corrective actions are prioritized and tracked as a part of a continuous corrective action program. The IP lists specific corrective actions, says who is responsible, and sets due dates. It is created by exercise leaders. It is discussed and validated during the AAM.

# Exercise Presentation Information

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

## Online Course

* A version of the exercise is available as a web-only course. This version can be opened on the FSIS website without the need to download anything.
* The key benefit of this option is that it is accessible to people with disabilities while including advanced features (e.g., interactive buttons, media, and 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 on-screen).

### 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 says 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 may be told to choose a button on-screen to go to a different page, instead of clicking Next or Back. In these cases, there will be on-screen 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.

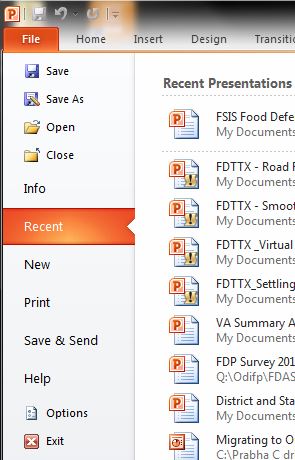
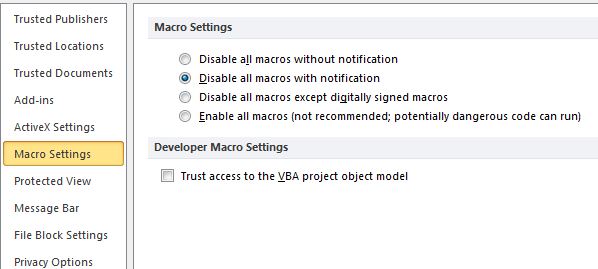
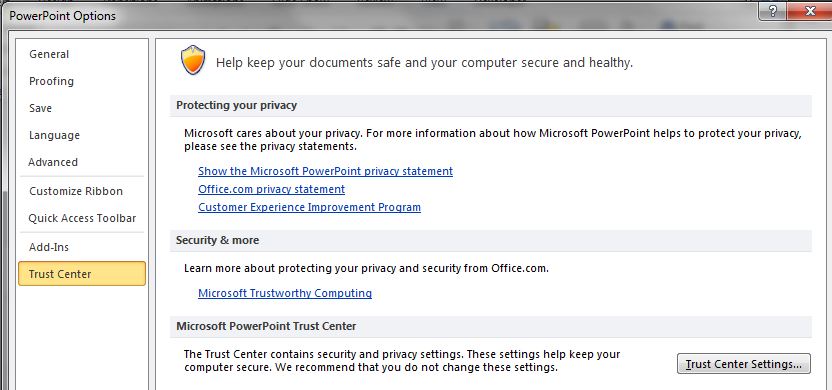
## PowerPoint

* This exercise can also be opened as four separate downloadable PowerPoint files. This version is more appropriate 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, you can customize the presentation to your particular situation. For example, where the original presentation refers to “a product that you produce,” you could insert 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 need to take notes by hand. Also, all players can see the answers as they are being typed, which may encourage additional thinking and suggestions.

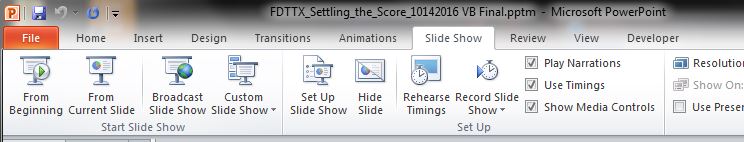
### PowerPoint Navigation

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

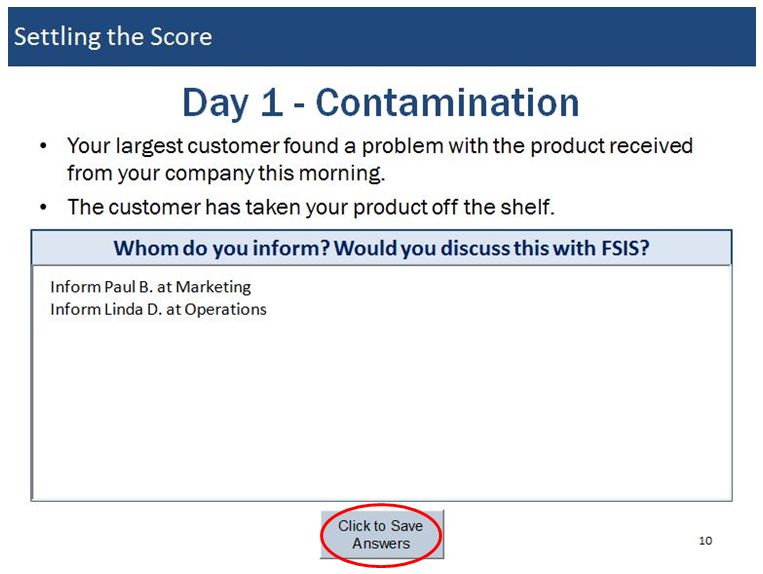
* Before starting the presentation, please enable macros in PowerPoint. This will allow you to use the full functionality of the presentation. In PowerPoint, click the **File** menu at top left, and then choose **Options** from the menu at left. In the dialogue box that opens, choose **Trust Center** 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. It 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 make a new document as described above.

# Appendix A: Exercise Schedule

| **Time** | **Personnel** | **Activity** | **Location** |
| --- | --- | --- | --- |
| **[Date]** | | | |
| [Time] | Exercise Leaders and Facilitator | Check-in for final instructions | [Location] |
| [Time] | Facilitators | Facilitators in starting positions | [Location] |
| [Time] | All | Players sign in | [Location] |
| [Time] | All | Facilitators brief players | [Location] |
| [Time] | All | Exercise starts | [Location] |
| [Time] | All | Exercise ends | [Location] |
| Immediately Following the Exercise | All | Hot Wash/turn in all participant feedback forms | [Location] |
| **[Date]** | | | |
| [Time] | Exercise leaders, facilitators | After Action Review | [Location] |

# Appendix B: Exercise Participants

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

# Appendix C: 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. The PowerPoint (PP) slide or Online Course (OC) page numbers for the scenario are listed. Use these to encourage talking and sharing, but try not to guide the discussion in a particular direction.

| 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. A disgruntled employee 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 may not be one you know or regularly test for.

The contaminant may 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. The PowerPoint (PP) slide or Online Course (OC) page numbers for the scenario are listed. Use these to encourage talking and sharing, but try not to guide the discussion in a particular direction.

| 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 information technology (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 * Cybersecurity 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 malicious 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. The PowerPoint (PP) slide or Online Course (OC) page numbers for the scenario are listed. Use these to encourage talking and sharing, but try not to guide the discussion in a particular direction.

| 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 assure 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, 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. The PowerPoint (PP) slide or Online Course (OC) page numbers for the scenario are listed. Use these to encourage talking and sharing, but try not to guide the discussion in a particular direction.

| 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 D: 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 |
| POC | Point of Contact |
| PP | PowerPoint |
| OC | Online Course |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |