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

**United States Department of Agriculture**

Situation Manual

[Date]

This Situation Manual (SitMan) gives participants all the tools needed for their roles in the exercise. Some exercise material is only for use by exercise planners, facilitators, and evaluators. Players may view other materials that are needed to perform well. All exercise participants may view the SitMan.

# Exercise Overview

|  |  |
| --- | --- |
| **Exercise Name** | Food Defense Preparedness and Recall Exercise Package (FD-PREP) |
| **Exercise Dates** | [Indicate the date(s) of the exercise] |
| **Scope** | This is a tabletop exercise planned for approximately 1 hour. It is meant 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** | **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[ ]  Cybersecurity[ ]  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 cybersecurity 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 here (i.e., establishment personnel, observers, others). Consider including the full list of participants 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**

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**

# General Information

## Exercise Objectives

The Objectives in Table 1 describe the expected outcomes for the exercise. The objectives for a particular exercise are selected by the exercise leaders.

|  |
| --- |
| **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.
* **Observers.** Observers do not directly engage in the exercise. But, they may inform player responses to the situation by asking questions or sharing expertise.
* **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.
* **Scribe**. The scribe takes notes during the exercise using the online course, 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 assumes your current state of readiness. Through the course of the exercise and the discussion questions, you may learn some things that will help you improve your future preparedness.

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 may even occur.
* Respond to the scenario using your knowledge of current plans and capabilities (i.e., you may 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 may 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 Evaluation

### Post-Exercise Debriefing or Hot Wash

When the exercise ends, leaders facilitate 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 be no longer than 30 minutes.

### Participant Feedback

Players will be asked to complete participant feedback forms. These provide players with the chance to freely comment on exercise activities and design. Participant feedback forms will be collected at the end of the Hot Wash.

### After Action Report and Improvement Planning

The After Action Report/Improvement Plan (AAR/IP) will be informed by participant feedback forms and facilitator notes. The AAR focuses on the analysis of Core Capabilities, including strengths, and areas to improve. The IP identifies corrective actions, assigns them to responsible parties, and sets target dates for completion.

# Participant Information and Guidance

## Exercise Rules

The following general rules govern exercise play:

* Real-world emergency actions take 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.
* Be at the appropriate site at least 30 minutes before the exercise starts. Wear the appropriate uniform and/or identification item(s).
* Sign in when you arrive.
* If you gain knowledge 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 may seem implausible. 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 After Action Meeting or Hot Wash at your venue with facilitators and controllers.
* Complete the Participant Feedback Form. This form allows you to comment candidly 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.

# 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, and 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 (PP:PowerPoint, OC: Online Course).

| Unit | Key Issues | Questions |
| --- | --- | --- |
| Welcome/ Intro | * Introduction
* Objectives
* Participant Roles
* Exercise Structure
 |  |
| Day 1PP 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 5PP 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 15PP 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 16PP 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 17PP 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 21PP 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 UpPP 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 (PP: PowerPoint, OC: Online Course).

| Unit | Key Issues | Questions |
| --- | --- | --- |
| Welcome/IntroPP Slides 1-8 OC Pages 1-8 | * Introduction
* Objectives
* Participant Roles
* Exercise Structure
 |  |
| Day 1PP 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 Information Technology (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 7PP 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 a 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 9PP 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 9PP 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 UpPP 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 (PP: PowerPoint, OC: Online Course).

| Unit | Key Issues | Questions |
| --- | --- | --- |
| Welcome/IntroPP Slides 1-8OC Pages 1-8 | * Introduction
* Objectives
* Participant Roles
* Exercise Structure
 |  |
| Day 1PP Slides 9-15OC 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 16-19OC 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 3PP Slides 20-26OC 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 4PP Slides 27-30OC 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 9PP Slides 31-33OC 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 12PP Slides 33-36OC 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 14PP Slides 37-39OC 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 UpPP Slides 40-44OC 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 (PP: PowerPoint, OC: Online Course).

| Unit | Key Issues | Questions |
| --- | --- | --- |
| Welcome/IntroPP Slides 1-8OC Pages 1-8 | * Introduction
* Objectives
* Participant Roles
* Exercise Structure
 |  |
| Day 1 – 9.00 AMPP Slides 9-17OC 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 18-20OC 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 AMPP Slides 20-22OC 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 AMPP 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 PMPP Slides 26-27OC 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 PMPP Slides 28-30OC 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 14PP Slides 31-33OC 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 UpPP Slides 35-39OC 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

| **Time** | **Personnel** | **Activity** | **Location** |
| --- | --- | --- | --- |
| **[Date]** |
| [Time] | Controllers and Facilitators | 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, Controllers, Facilitators  | After Action Review | [Location] |

# Appendix B: Exercise Participants

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

# Appendix C: Acronyms

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

# Appendix D: Participant Feedback Form

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

**Exercise Date:**

Please enter your responses below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name:** |  | **Title:** |  |
| **Organization:** |  |  |  |  |
| **Role:**  | Participant [ ]  | Facilitator *[ ]*  | Observer *[ ]*  | Evaluator *[ ]*  |
| **Exercise Scenario:** |  |

## Part I: Recommendations and Corrective Actions

1. Based on what you learned today, list the top three strengths and/or areas that need improvement.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

## Part II: Assessment of Exercise Design and Conduct

Please rate your level of agreement with each statement below on the scale provided.

| **Assessment Factor** | **Strongly****Disagree** | **Strongly Agree** |
| --- | --- | --- |
| The exercise was well structured and organized. | 1 | 2 | 3 | 4 | 5 |
| The exercise scenario was realistic. | 1 | 2 | 3 | 4 | 5 |
| The facilitator/controller(s) was knowledgeable about the area of play.  | 1 | 2 | 3 | 4 | 5 |
| The facilitator/controller(s) kept the exercise on target. | 1 | 2 | 3 | 4 | 5 |
| The handouts helped me prepare for and participate in the exercise. | 1 | 2 | 3 | 4 | 5 |
| Participating in the exercise was appropriate for someone in my position. | 1 | 2 | 3 | 4 | 5 |
| The participants included the right people in terms of level and mix of disciplines. | 1 | 2 | 3 | 4 | 5 |
| This exercise helped my team to practice and improve the capabilities that were tested. | 1 | 2 | 3 | 4 | 5 |
| After this exercise, I believe my team is better prepared to properly deal with the scenario that was practiced. | 1 | 2 | 3 | 4 | 5 |

## Part III: Participant Feedback

How could this exercise or future exercises be improved?

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |