UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE
WASHINGTON, DC

FSIS DIRECTIVE

5420.1
Rev. 11

9/26/23

FOOD DEFENSE TASKS AND THREAT NOTIFICATION RESPONSE PROCEDURES FOR THE OFFICE OF FIELD OPERATIONS

I. PURPOSE

This directive provides instructions to conduct food defense activities assigned to inspection program personnel (IPP) at meat (including Siluriformes fish and fish products) and poultry establishments, egg product plants, and import inspection establishments. Food defense activities include performing food defense tasks and observing and reporting food defense vulnerabilities. This directive also outlines the internal FSIS communication protocol for addressing threats to the food and agriculture sector. This directive has been updated to replace references to the Office of Data Integration and Food Protection (ODIFP) with the Office of Management's (OM), Significant Incident Preparedness and Response Staff (SIPRS) role in the threat notification process, and minor updates to the Food Defense Memorandum of Interview (MOI) instructions. This directive has also been revised to update where to find resources and references to egg products.

II. CANCELLATION

FSIS Directive 5420.1, Revision 10, *Food Defense Verification Tasks and Threat Notification Response Procedures for the Office of Field Operations*, 3/13/17

III. BACKGROUND

A. Food defense is the protection of food products from intentional contamination or adulteration intended to cause public health harm or economic disruption. FSIS promotes food defense by encouraging establishments to voluntarily adopt a functional Food Defense Plan (FDP), implement food defense practices, and conduct training and exercises to ensure preparedness. Food defense practices are policies, procedures, or countermeasures to mitigate vulnerability to intentional contamination. IPP perform food defense tasks to identify vulnerabilities within establishments that may lead to intentional contamination of FSIS-regulated product.

B. A functional FDP can help an establishment prevent, protect, mitigate, respond to, and recover from, an intentional contamination incident. The absence of a functional FDP may increase an establishment's vulnerability to intentional contamination because important security measures needed to protect the facility, product, and employees may not be in place. Functional FDPs are voluntary in official FSIS-regulated establishments (i.e., not mandated by regulation); however, FSIS encourages establishments to adopt a functional FDP to further protect their product. If establishments choose to develop a functional FDP, they are not required to share it with IPP.

IV. NOTIFICATION OF THREAT FROM INTELLIGENCE COMMUNITY

A. IPP are to know the protocol for communicating threat information related to the food and agriculture sector to establishment management through proper supervisory channels as necessary. Threat information from the intelligence community is to be communicated through the following:

1. The SIPRS Director or designee is the primary point of contact for receipt of threat information from the intelligence community;

2. If a threat has the potential or is expected to affect food or agriculture, the SIPRS Director or designee is to inform the FSIS Administrator and FSIS Management Council;

3. The SIPRS Director or designee is to determine the appropriate distribution of the threat information and coordinate with the FSIS Office of Management (OM), Office of Field Operations (OFO), Office of Investigation, Enforcement and Audit (OIEA), Office of Public Affairs and Consumer Education (OPACE), Office of International Coordination (OIC), and Office of Public Health Science (OPHS) to notify employees, stakeholders, and the public, as appropriate; and

4. In the event of a significant incident, the FSIS Emergency Management Committee may be alerted or activated and other response actions taken pursuant to FSIS Directive 5500.2, *Significant Incident Response*.

B. As soon as OFO supervisory personnel are notified of threat information, they are to inform establishment management of the alert. IPP are to document their discussion with establishment management in a MOI (see FSIS Directive 5010.1, *Food Safety Related Topics During Weekly Meetings*).

C. The SIPRS Director or designee is to notify the OM Assistant Administrator/Deputy Assistant Administrator (AA/DAA), the FSIS Administrator, and the FSIS Management Council of any changes in threat information, to include when the period of concern has expired. The SIPRS Director or designee is to coordinate with OFO, OIEA, OPACE, OIC, and OPHS to notify employees, stakeholders, and the public, as appropriate. Supervisory personnel are to advise other IPP in the establishment and establishment management of the change in threat status.

D. If IPP observe a potentially significant incident that presents a grave, or potentially grave, threat to public health or to the safety of FSIS-regulated product or to personnel, they are to report it through supervisory channels. IPP are to follow instructions provided in FSIS Directive 5500.2, which also lists examples of significant incidents.

V. PERFORMING FOOD DEFENSE TASKS IN PHIS

A. IPP are to perform food defense tasks as assigned in PHIS. PHIS will automatically generate one routine food defense task per quarter to the establishment task list. Inspectors-in-charge (IICs) assigned to multi-inspector, multi-shift establishments are to use the established information-sharing practices to ensure that they perform the food defense task at the prescribed frequency. The FLS is to provide any necessary oversight. While performing this task, if IPP identify that the establishment profile information on the food defense plan is not current, IPP are to update the profile to reflect the status of the establishment's food defense plan.

B. The table below lists the questions associated with the food defense task. The examples of food defense practices provided in the table are not all-inclusive. Establishments can implement a variety of food defense measures to protect their products, people, and processes from intentional contamination. Food defense is not a one-size-fits-all approach. IPP are to consider this when performing the food defense task. In addition, some food defense activities may not be obvious to IPP. Therefore, IPP are to discuss these activities with management during the weekly meeting to learn more about the establishment's food defense practices. IPP are to be aware that establishments can use the FSIS Food Defense Risk Mitigation Tool to find a more comprehensive list of food defense practices (mitigation strategies). If IPP have questions regarding this task, they are to direct them to their immediate supervisor.
C. IPP are to answer all the questions in the food defense PHIS questionnaire as either "Yes," "No," or "not applicable" ("N/A"). IPP are not to leave questions blank.

D. As IPP are completing the task, they are to be aware that food defense practices are policies, procedures, or countermeasures to mitigate vulnerability to intentional contamination. An establishment does not have to implement multiple food defense practices for IPP to answer "Yes" to the task questions. IPP are to answer "Yes" to the question if one or more of the examples of food defense practices are implemented or if there is another mitigation strategy to address the potential vulnerability. If IPP have questions about the appropriateness of a mitigation strategy that is not listed as an example, they are to direct these questions to their immediate supervisor.

E. Not all tasks may be applicable to all establishment types. If a task does not apply to their establishment, IPP are to answer "N/A."

F. IPP are to try to observe as many of the food defense practices as possible. However, if IPP do not know the answer to a question, they are to discuss it with establishment management at a weekly meeting. In this case, the IPP are to leave the task open until the next weekly meeting and complete the task after that meeting. The establishment is not required to disclose information about its food defense practices to IPP. IPP are not to issue a Noncompliance Record (NR) if the establishment chooses to withhold information. If IPP do not know the answer to a question and are unable to verify the answer with establishment management, they are to answer it as "N/A."

G. If IPP are unclear as to how to conduct the food defense task or have questions about the task, they are to contact their immediate supervisor. Supervisors seeking support or guidance are to submit questions to the SIPRS at FoodDefense@usda.gov.

Task Question	**Examples of Food Defense Practices (not all-inclusive)**	**Additional Information**
1. Does the establishment implement practices to prevent unauthorized access to the facility?	• Locked doors • Fence around perimeter of facility • Security guards • Alarm system • Controlled-access system	This question is targeting practices the establishment has in place to prevent an unauthorized individual from getting into or having access to the facility.
2. Does the establishment implement practices to prevent access to restricted areas inside the facility? *Restricted areas are secure areas where the*	• Surveillance cameras • Designate and clearly mark all restricted areas • Controlled-access system • Locks • Buddy system	The definition of a restricted area may differ from one establishment to another. Examples of restricted areas may include: areas where ingredients, chemicals, or hazardous materials are stored; in-plant laboratory; areas where

Task Question	Examples of Food Defense Practices (not all-inclusive)	Additional Information
establishment wants to control access.	• Restrict access to ice and storage tanks for potable water and water reuse systems	product containers or processing equipment is stored; etc.
3. Does the establishment implement personnel security measures to prevent an intentional contamination incident?	• Background checks • Employee identification system (e.g., badges, color-coded uniforms) • Restrict personal items in operational areas (e.g., cell phones, cameras) • Restrict temporary employees and non-employees to areas relevant to their work • Maintain updated shift roster	Personnel security measures are actions the establishment can take either before or after an employee is hired to ensure there is no history of behavior or current behaviors that may indicate an individual is likely to intentionally contaminate product or negatively impact public health or the safety of others.
4. Does the establishment implement management controls to prevent intentional contamination?	• Maintain a policy for handling suspect persons/disgruntled employees, items, and events • Adopt a functional food defense plan • Track customer complaints/comments for trends • Maintain a system to encourage employees to report signs of possible product contamination, unknown or suspicious persons in the facility, or other food defense vulnerabilities • Conduct mail-handling activity in a separate room or facility that is away from in-plant food production/processing operations	Management controls are activities that establishment management can do to reduce the likelihood of intentional contamination.
5. Does the establishment promote situational awareness for employees, including: • Training on food defense? • Procedures for reporting suspicious activity?	• Food defense training methods may include (but are not limited to) online, in-person, fact sheets, or in-plant exercises • Employees should be encouraged to report signs of possible product contamination, unknown or suspicious persons in the facility, or other food defense vulnerabilities	The following free training courses and exercise toolkits are available for industry: • Food Defense and Recall Preparedness Exercise Tool (FSIS) • Employees FIRST (FDA) • Food Defense 101 (including ALERT) (FDA)

Task Question	Examples of Food Defense Practices (not all-inclusive)	Additional Information
6. Does the establishment implement practices to prevent unauthorized access to computer systems or industrial control systems?	• Protect computer systems through firewalls and passwords • Maintain updated computer virus detection systems • Provide information security training to employees with access to cyber systems • Limit or closely monitor remote access to web-based applications that manage industrial control systems	An industrial control system is an integrated hardware and software system designed to monitor and control the operation of machinery and associated devices within the food production environment. Industrial control systems may include (but are not limited to): • Supervisory control and data acquisition (SCADA) systems • Distributed control systems • Programmable logic controllers The following cyber resources are available for industry: • NIST.gov/CyberFramework • US-CERT.gov • StaySafeOnline.org • FSIS Cybersecurity Countermeasures ○ Select Cybersecurity Countermeasures in the Lookup Tool
7. Does the establishment implement practices for the following processing activities: • Mixing, blending, and similar activities (e.g., coating/mixing/ grinding/rework)? • Non-meat, non-poultry, and non-egg ingredient handling (e.g., ingredient staging/prep/addition)? **Answer N/A if this is an import establishment*	• Restrict access • Conduct monitoring and surveillance • Verify product integrity throughout the production process, up to primary and secondary packaging	• These processing activities are those that have been identified as being more vulnerable to intentional contamination. • Non-meat and non-egg ingredients may include (but are not limited to) spices, preservatives, flavoring, etc.
8. Does the establishment implement practices for reinspection/staging areas? **Answer N/A if re-inspection does not occur at the establishment*	• Restrict access • Conduct monitoring and surveillance • Verify primary and secondary packaging is intact • Maintain updated product inventory	
9. Does the establishment implement practices to	• Maintain access log • Restrict access	

Task Question	Examples of Food Defense Practices (not all-inclusive)	Additional Information
prevent access to storage of the following items: • Raw materials and non-meat, non-poultry, and non-egg ingredients (e.g., spices, preservatives)? • Liquid storage and handling (e.g., marinade, brine, open vats/bins/silos/totes)? • Chemicals and hazardous materials? • Finished products (ready to be shipped)? • Labels and packaging materials?	• Conduct monitoring and surveillance • Control product labels and packaging to prevent theft and misuse	
10. Does the establishment implement practices for the following shipping and receiving activities: • Bulk liquid receiving/loading? • Procedures for incoming product integrity? • Verifying transportation vendors and drivers?	• Control access • Ensure seals and locks are present • Verify boxes or containers have not been tampered with • Background checks on transportation drivers • Driver identification upon pick-up/delivery • Minimize the time a truck is unlocked during loading or delivery	
11. Does the establishment have incident response procedures in place in the event a contamination incident occurs?	• Pre-established communication with local, state, and federal law enforcement or incident response personnel • Recall plan • Procedures to communicate with the media or consumers • Have up-to-date establishment layout/blueprints for local law enforcement, including the fire department, if needed • Maintain records to allow easy trace-back of raw materials to suppliers • Maintain records to allow easy trace-forward of finished products to vendors	In most cases, it cannot be determined if a contamination event is intentional or unintentional until later in the investigation. Therefore, incident response procedures for both intentional and unintentional contamination incidents should be considered when answering this question.

Task Question	Examples of Food Defense Practices (not all-inclusive)	Additional Information
12. Has the establishment conducted a written vulnerability assessment of their facility within the past year?		A vulnerability is a weakness within the food production process that makes it easy to intentionally contaminate product. A vulnerability assessment is an assessment to identify vulnerabilities within or outside of a facility that may lead to intentional contamination of product.
13. Additional comments?		This question allows IPP to enter free text to provide further explanation or clarification for answers to the task questions.

H. To access and complete the PHIS task questionnaire, IPP are to:

1. Look for “Food Defense Task” on the establishment task list and schedule it on their task calendar, then claim the task when they are ready to conduct the task;

2. Select the “Activity” tab, then select the applicable Verification Activity (Review & Observation, Record Keeping, or Both);

3. Select the “Questionnaire” tab. Click on “Take Questionnaire” tab to access the questions;

4. Click “Start” to begin questionnaire;

5. Select answers to questions on page one. Click “Next” and proceed to the next page of questions. IPP are to complete all questions and are not to leave any blank or unanswered. IPP are to select “N/A” if the question does not apply to the establishment or If IPP do not know the answer to a question and are unable to verify the answer with establishment management;

6. Click "Submit” to complete the questionnaire; and

7. Record the task as completed after the questionnaire results have been entered.

I. IPP are to review the answers of the questionnaire with establishment management in the weekly meeting following task completion. Based on the questionnaire answers, IPP are to discuss areas in the establishment where a food defense vulnerability exists and mitigation strategies to address identified vulnerabilities and weaknesses in the establishment. IPP can find examples of common food defense mitigation strategies in FSIS Food Defense Risk Mitigation Tool.

J. When a threat notification is issued, the IIC is to receive specific instructions through supervisory channels on other actions, if any, that they are to take based on information received about the threat to a product or process. If additional food defense tasks are necessary, IPP are to follow the instructions in FSIS Directive 13,000.1, *Scheduling In-Plant Inspection Tasks in the Public Health Information System (PHIS)*, when scheduling a directed PHIS task.

K. If the establishment requests guidance or additional information on food defense, including how to develop a functional FDP, IPP are to direct establishments to http://www.fsis.usda.gov/fooddefense. The food defense website contains guidance documents and tools to assist establishments with food defense practices (e.g., a general FDP template, brochures, guides, and fact sheets). Many of these materials are available in multiple languages. Alternatively, IPP may download a copy of the General Food Defense Plan from the FSIS website at http://www.fsis.usda.gov/fooddefense.

VI. OBSERVE AND DOCUMENT FOOD DEFENSE VULNERABILITIES

A. IPP are to document vulnerabilities observed while performing a food defense task or during daily inspection activities when there is no evidence of product adulteration. IPP are to document their findings in a Food Defense MOI after discussing them with establishment management. IPP are to provide a finalized copy of the Food Defense MOI to establishment management. IPP are only to document observed vulnerabilities in a Food Defense MOI, not every observation made.

B. IPP are to document Food Defense MOIs by selecting Inspection Verification >> Select Establishment >> Memorandum of Interview from the left toolbar of the PHIS homepage. IPP can also document food defense MOIs when completing a food defense task when saving the inspection task with a non-regulatory concern checked. Once the task is saved, click on the "Create/Edit MOI" button.

1. To document a domestic OFO Food Defense MOI, click on "Add Food Defense OFO" to open the "Domestic Food Defense MOI" page to access key functions of the MOI.

    a. In the "Status" tab left-click on the attendee's name. To select more than one attendee, hold "Ctrl" on the keyboard while left-clicking on each applicable name. In the "Category" tab, select the category of potential vulnerability (No product adulteration observed). For "Occurrence", choose either the 1st, 2nd, or 3rd time this vulnerability has been observed.

    b. In the "Product" tab, leave this tab blank;

    c. In either the "Processing" or "Storage" tab, identify the vulnerability point or concern. Additional vulnerabilities, other than those related to processing and storage activities, are available for selection in these tabs;

    d. Check the "Finalize" box and then click "Save" to complete the Food Defense MOI (FSIS Form 5420-1). At the next weekly meeting, provide a finalized copy of the Food Defense MOI to establishment management. Discuss the food defense findings with management, including proposed mitigation actions, and document in the weekly meeting memorandum; and

    e. If the same vulnerability is observed a 4th time, IPP are to notify the District Office through supervisory channels.

2. To document an import Food Defense MOI click on "Add Food Defense OIA" to open the "Import Food Defense MOI" page to access key functions of the MOI.

    a. In the "Status" tab, select category of potential vulnerability (No product adulteration observed), occurrence (1st, 2nd, or 3rd), and attendees with a left mouse click on attendee's name. To select more than one attendee, hold "Ctrl" on keyboard while left clicking on each applicable name;

b. In the “Product” tab, leave this box blank;

c. In either the “Processing” or “Storage” tab, indicate the vulnerability point or concern. Note: Additional vulnerabilities, other than those related to processing and storage activities, are available for selection in these tabs;

d. Check the “Finalize” box and then click “Save” to complete the Food Defense MOI (FSIS Form 5420-1). At the next weekly meeting, provide a finalized copy of the Food Defense MOI to establishment management. Discuss potential mitigation strategies for the vulnerabilities and document the discussion in the weekly meeting memorandum; and

e. If the same vulnerability is observed a 4th time, IPP are to notify the District Office through supervisory channels.

C. When IPP perform a food defense task or perform other daily inspection activities and find a food defense vulnerability or concern, and there is evidence of product adulteration (e.g., regulatory noncompliance), IPP are to schedule and perform a directed Hazard Analysis and Critical Control Point (HACCP), Sanitation Standard Operating Procedures (SOP), or other appropriate inspection task to record the observed noncompliance citing the applicable regulation. IPP are to:

1. Immediately retain the affected product by attaching a U.S. Retain tag, then notify establishment management and discuss the findings;

2. After informing establishment management, IPP are to report any potentially significant incidents through supervisory channels;

3. Add the appropriate inspection verification task according to FSIS Directive 13,000.1 to the task calendar, perform the task, and document the observed product contamination in an NR. IPP are to cite the applicable regulation in accordance with FSIS Directive 5000.1, *Verifying an Establishment’s Food Safety System;*

4. Complete a Food Defense MOI; and

5. Immediately provide a finalized copy of the MOI to establishment management and inform management that an NR will also be issued describing the adulterated product and potential vulnerability or concern.

VII. FOOD DEFENSE TASKS IN FACILITIES PAYING FEES FOR INSPECTION SERVICE (VOLUNTARY INSPECTION)

IPP in facilities that only have services as outlined in 9 CFR Parts 350, 351, 352, 354, or 592, are not assigned routine food defense tasks. However, these facilities are encouraged to develop a functional FDP. If the facility requests guidance or additional information on food defense, including how to develop a functional FDP, IPP are to direct establishments to http://www.fsis.usda.gov/fooddefense.

VIII. SUPERVISORY RESPONSIBILITIES

A. “Supervisory personnel” refers to any OFO personnel that supervise IPP who conduct food defense activities.

B. The supervisor plays a key role in ensuring that decisions made by IPP are consistent with FSIS statutory authority and Agency policy, and that duties are performed in accordance with prescribed inspection methods and procedures addressed in this directive.

C. FSIS supervisory personnel are to discuss the key points identified in this directive with IPP.

D. Supervisory personnel are to ensure that IPP are correctly applying the methodology presented in this directive, making informed decisions, properly documenting findings, and taking the appropriate enforcement actions as instructed in this directive.

E. Supervisory personnel are to refer to the current version of the FSIS Directive 4430.3, *In-Plant Performance System (IPPS).*

IX. DATA ANALYSIS

SIPRS will work with OPARM to analyze food defense task data, as needed, to determine trends in food defense practices being implemented by establishments. Results will help to inform activities to further protect public health and mitigate food defense vulnerabilities.

X. QUESTIONS

Refer questions regarding this directive to SIPRS by email at FoodDefense@usda.gov.

Assistant Administrator
Office of Policy and Program Development