

Food Defense

OBJECTIVES

After completion of this module, the participant will be able to:

1. Explain the risk that intentional contamination presents to FSIS-regulated products.
2. Define the following terms:
 - a. Food safety
 - b. Food defense
 - c. Food defense practices
 - d. Supply chain
 - e. Food defense vulnerability
3. List the characteristics of a functional food defense plan.
4. Recognize examples of vulnerabilities and associated food defense practices.
5. Describe the purpose of the food defense task.
6. Identify measures an establishment can take to protect their product from intentional contamination.
7. Explain how inspectors are to perform the Food Defense task and document food defense vulnerabilities in the Public Health Information System (PHIS).

REFERENCES

1. Directive 5420.1_Rev 10, "Food Defense Tasks and Threat Notification Response Procedures for the Office of Field Operations"
2. FSIS – [Food Defense and Emergency Response](#) webpage
3. FSIS – [Food Defense Risk Mitigation Tool](#) webpage
4. The Centers for Disease Control; Disease Category webpage
5. FDA – [FDA Food Defense](#) webpage

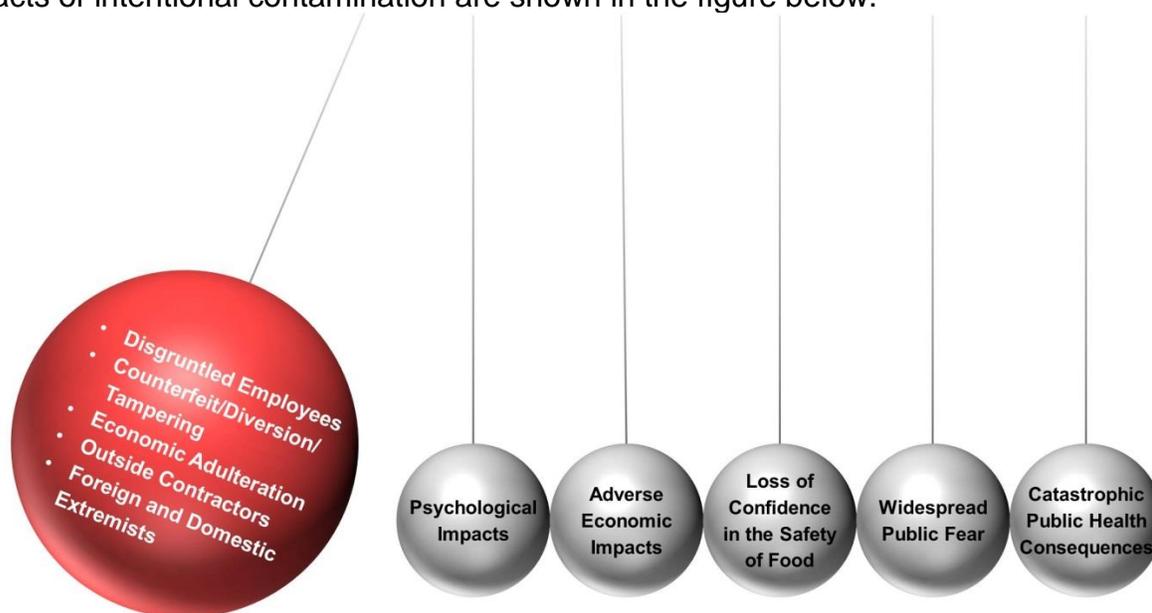
INTRODUCTION

This module will address food defense activities in FSIS by providing some background on food defense, discussing common food defense vulnerabilities and mitigation strategies, and then explaining your role and inspection activities that are related to food defense.

Prior to September 11, 2001, FSIS focused primarily on protecting meat, poultry, and egg products from unintentional contamination. The events of September 11, 2001, brought the issue of the vulnerability of our food supply to the forefront and called for the food and agriculture sector to focus on food defense.

FSIS' mission is to ensure that the Nation's commercial supplies of meat, poultry, and egg products are safe, wholesome, and correctly labeled and packaged, as required by the Federal Meat Inspection Act, the Poultry Products Inspection Act, and the Egg Products Inspection Act. The Public Health Security and Bioterrorism Act of 2002 established that FSIS could utilize existing authorities to give high priority to enhancing and expanding the capacity to conduct activities to enhance the ability of the agency to inspect and ensure the safety/wholesomeness of meat, poultry, and egg products.

Food defense is the protection of food products from contamination or adulteration intended to cause public health harm or economic disruption. Potential sources and impacts of intentional contamination are shown in the figure below.



Potential **Sources** & Impacts of Intentional Adulteration

The [Significant Incident Preparedness & Response Staff](#) (SIPRS) is responsible for managing all food defense activities for the Agency. SIPRS works with government agencies at all levels, industry, and other organizations to develop and implement strategies to prevent, protect against, mitigate, respond to, and recover from intentional contamination of the food supply

The Significant Incident Preparedness & Response Staff is available at any time to answer questions related to food defense and can be reached via email at: SIPRS@usda.gov.

FOOD DEFENSE TERMINOLOGY

In order to prevent, protect against, mitigate, respond to, and recover from threats and hazards of great risk to the food supply, it is important that preparedness efforts incorporate food safety, food defense, and food security. While there are distinct differences between these three concepts, a comprehensive approach that addresses food safety, food defense, and food security considerations improve resilience and protect public health. We need to understand what these terms means:

Food Security – When all people at all times have both physical and economic access to enough food for an active, healthy life. Food security includes both physical and economic access to food that meets people's dietary needs and food preferences. Therefore, the concept of food security certainly includes but encompasses much more than the idea of *food defense*.

Food Safety – means guarding against unintentional contamination of food. HACCP plans and Sanitation SOPs, which are developed based on what can be predicted to happen if we do not put safety measures at critical points, are used to guard against unintentional contamination.

Food Defense – is the protection of food products from intentional contamination or adulteration intended to cause public health harm or economic disruption. Food Defense is an integral part of FSIS' mission in protecting public health. The mission of the FSIS Food Defense Program is to protect the U.S. food supply from dynamic and evolving threats.

Other definitions important for our discussion include:

Food defense practices – policies, procedures, or countermeasures to mitigate vulnerability to intentional contamination.

Critical Infrastructure – The Patriot Act of 2001 defined critical infrastructures as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. The Food and Agriculture Sector is one of 16 critical infrastructures identified by the Patriot Act.

Supply Chain – continuous process including every step involved in food production and food reaching the consumer; often referred to as farm-to-table or farm-to-fork.

FOOD DEFENSE VULNERABILITIES AND FOOD DEFENSE PRACTICES

A **vulnerability** can be any part of the food production or storage system where a protective measure should be implemented to protect a product from intentional adulteration, but such a measure is found to be missing or not in place.

Food defense vulnerabilities are weaknesses within the food production process that make it easy to intentionally contaminate product. Examples of food defense vulnerabilities may include (please note this list is not all-inclusive):

- Unsecured entrances
- Poor lighting around the facility
- Failing to control access and properly secure restricted areas inside the facility, including access to processes and/or ingredients that may be more vulnerable to intentional contamination (e.g., spices, preservatives, marinade, brine, etc.)
- Failing to control product labels and packaging to prevent theft and misuse
- Ensuring seals and locks are present, where appropriate (e.g., bulk liquid loading/storage/transport activities, chemicals and hazardous materials, etc.)
- Lack of or insufficient personnel security measures (e.g., background checks, employee ID badges, delivery driver/vendor identification, etc.)
- No system for employees to report suspicious behavior
- Computer systems and/or control systems that lack appropriate security measures that may lead to a cyber security incident (e.g., passwords, firewalls, virus protection)

An establishment can put **food defense practices** (also called mitigation strategies) into place to reduce the likelihood that intentional contamination will occur. **Food defense is not a one-size-fits-all approach!** Food defense practices that are implemented to protect products within a large establishment may not be effective or

needed in a small or very small establishment. This should be considered when inspection program personnel (IPP) conduct their food defense activities.

Examples of food defense practices may include (not all-inclusive):

- Locked doors
- Surveillance cameras
- Security guards
- Alarm system
- Controlled-access system
- Designate and clearly mark all restricted areas
- Perform background checks on new employees
- Restrict personal items in operational areas
- Employee identification system
- Maintain an anonymous system for reporting suspicious behavior
- Conduct food defense training for employees
- Protect computer systems and automated systems with firewalls and passwords

A more comprehensive list of mitigation strategies for various components of the food supply can be found in FSIS' [Food Defense Risk Mitigation Tool](#).

FOOD DEFENSE IN FSIS-REGULATED ESTABLISHMENTS

Food defense is voluntary for FSIS-regulated establishments. This means that FSIS does not have regulatory authority when it comes to food defense. Even though food defense is voluntary, FSIS encourages establishments to protect their products from intentional contamination by doing the following:

- Implementing food defense practices,
- Conducting training and exercises to ensure preparedness, and
- Adopting a functional food defense plan

A functional food defense plan is an approach to identify and mitigate vulnerabilities; it can help an establishment prevent, protect against, respond to, and recover from an intentional contamination incident. A food defense plan is functional when it meets all four of the following criteria:

1. Developed – the plan is documented and signed
2. Implemented – food defense practices identified in the plan are actually implemented

3. Tested – food defense measures are monitored and validated to ensure they are working
4. Reviewed and maintained – the plan is reviewed at least annually and revised as needed.

Note: An establishment must be **implementing** the elements of its food defense plan in order for FSIS to consider it “functional.”

The absence of a functional food defense plan 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. Even though functional food defense plans are voluntary, FSIS considers such plans to be an important tool that can reduce the risk of intentional adulteration of food products.

An establishment does not have to provide IPP access to its food defense plan or any associated documents (e.g., employee personnel files). It is beneficial if IPP are permitted access to the plan, as it may be useful in identifying how the establishment is addressing food defense. If the establishment shares its plan, IPP are not to keep or make copies of the written plan. IPP also cannot show or share anything about the plan with any outside source because it includes sensitive security information.

IPP are responsible for maintaining the functional food defense plan status for an establishment in the Establishment Profile in PHIS. Food defense plan status can be found on the “General” page → “Other” tab in the Establishment Profile. IPP are to check the box for “Written food defense plan” if the establishment meets **ALL** four criteria for having a functional food defense plan. This status should be updated per the frequency identified in Directive 5300.1, *Managing the Establishment Profile in the Public Health Information System*, or when IPP become aware of a change in the establishment’s functional food defense plan status.

If an establishment does not have a food defense plan, they can access the [FSIS General Food Defense Plan](#) template on the FSIS website. (See Attachment 1) The Agency has additional food defense guidance documents (e.g. worksheets, checklists, and fact sheets) for consumers, industry, and state and local agencies. All of these materials are also available on the FSIS webpage, under [Food Defense and Emergency Response](#).

NATIONAL TERRORISM ADVISORY SYSTEM

The National Terrorism Advisory System (NTAS) is a system managed by the Department of Homeland Security (DHS) to communicate information about terrorist threats by providing information to the American public. Under the NTAS system, DHS coordinates with other federal entities to issue formal alerts when the Federal government receives information about a specific or credible terrorist threat.

If there is specific and credible information about a terrorist threat against the U.S., DHS will share the NTAS alert with the American public when circumstances are justified. These alerts include a clear statement that there is an “elevated threat” or “imminent threat”.

- Elevated threat: if there is credible threat information, but only general information about timing and target such that it is reasonable to recommend implementation of protective measures to thwart or mitigate against an attack.
- Imminent: there is a belief that the threat is credible, specific, and impending in the very near term.

The NTAS alerts are based on the nature of the threat including the geographic region, mode of transportation, or critical infrastructure potentially affected by the threat. The alerts also provide a concise summary of the potential threat, information about actions being taken to protect public safety, and recommended steps that individuals, communities, businesses, and governments can take.

FSIS DIRECTIVES

There are five FSIS Directives related to food defense:

- 5420.1 – Food Defense Tasks and Threat Notification Response Procedures for the Office of Field Operations
- 5420.3 – Food Defense Surveillance Procedures and National Terrorism Advisory System Alert Response for the Office of Investigation, Enforcement and Audit
- 5500.2 – Significant Incident Response
- 5500.3 – Incident Investigation Team Reviews
- 5500.4 – Products Intentionally Adulterated with Threat Agents

Directive 5420.1 outlines the duties that are relevant to the in-plant inspection team when performing the food defense task and observing/reporting food defense vulnerabilities. The other directives cover food defense duties for other FSIS personnel. Depending on the role of the in-plant inspector, you should familiarize yourself with these other important directives, if it applies to your duties.

FSIS DIRECTIVE 5420.1

Let us look at Directive 5420.1 in more detail. First, this directive describes the PHIS **Food Defense task** and its frequency. The directive also discusses threat notification procedures that the Office of Field Operations (OFO) is to follow in the event FSIS receives threat information related to the food and agriculture sector.

Threat Notification

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, such as an NTAS bulletin or alert from the intelligence community is to be communicated through the following:

1. The FSIS Significant Incident Preparedness and Response Staff (SIPRS) Chief Operating Officer (COO) 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 COO informs the FSIS Administrator and FSIS Management Council;
3. The SIPRS COO determines the appropriate distribution of the threat information and coordinates with other FSIS offices to notify employees, stakeholders, and the public, as appropriate; and
4. In the event of a significant incident, the FSIS Emergency Management Committee (EMC) may be alerted and other response actions taken pursuant to [FSIS Directive 5500.2 Significant Incident Response](#)

Supervisory personnel are to ensure that any notifications distributed to field employees are available to IPP in the establishment. As soon as 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 memorandum of interview (MOI) (see [Food Safety Related Topics For Discussion During Weekly Meetings With Establishment Management](#)). 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](#).

If there is a specific threat, additional Food Defense tasks may be necessary. Additional actions may be needed to reduce the threat of intentional adulteration of food products. IPP must clearly understand their roles and what will be required of them to respond properly to that threat.

Performing Food Defense Tasks in PHIS

IPP in meat and poultry establishments are to perform the “Food Defense task” as assigned in PHIS. PHIS will automatically generate one routine Food Defense task per quarter to the establishment task list. This task has a priority 3 in the Establishment Task List including a start/end date window of three months. Only one questionnaire is to be completed per establishment. The task is to only be performed on one shift in multi-shift establishments. The supervisor should determine which shift performs the task. The shift that does not complete the task should mark the task as not performed with a justification of ‘Task assigned to another inspector.’

IPP perform the Food Defense task to identify vulnerabilities within establishments that may lead to intentional contamination of FSIS-regulated products.

There are resources that the IPP can use as an aid to assess vulnerabilities while performing the Food Defense task. These resources can be found on FSIS’ food defense webpage (<https://www.fsis.usda.gov/wps/portal/fsis/topics/food-defense-defense-and-emergency-response>) under “Tools, Resources, and Training”.

To perform the food defense task in PHIS, IPP are to:

1. Schedule the Food Defense Task to the PHIS task calendar;
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. Answer all the questions – IPP 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 they

do not know the answer to the question. IPP are to answer “Yes” if there is another mitigation strategy addressing the potential vulnerability;

6. Click “Submit” to complete the questionnaire; and
7. Record the task as completed after the results have been entered.

Prior to completing the questionnaire, IPP should discuss food defense activities with management during a weekly meeting to learn more about the establishment’s food defense practices. This will allow them to accurately complete the questionnaire.

IPP are to discuss the answers of the questionnaire with establishment management in the weekly meeting following task completion, including areas in the establishment where food defense vulnerability exists, as well as food defense practices. IPP can use the Food Defense Risk Mitigation Tool in their discussion with establishment management.

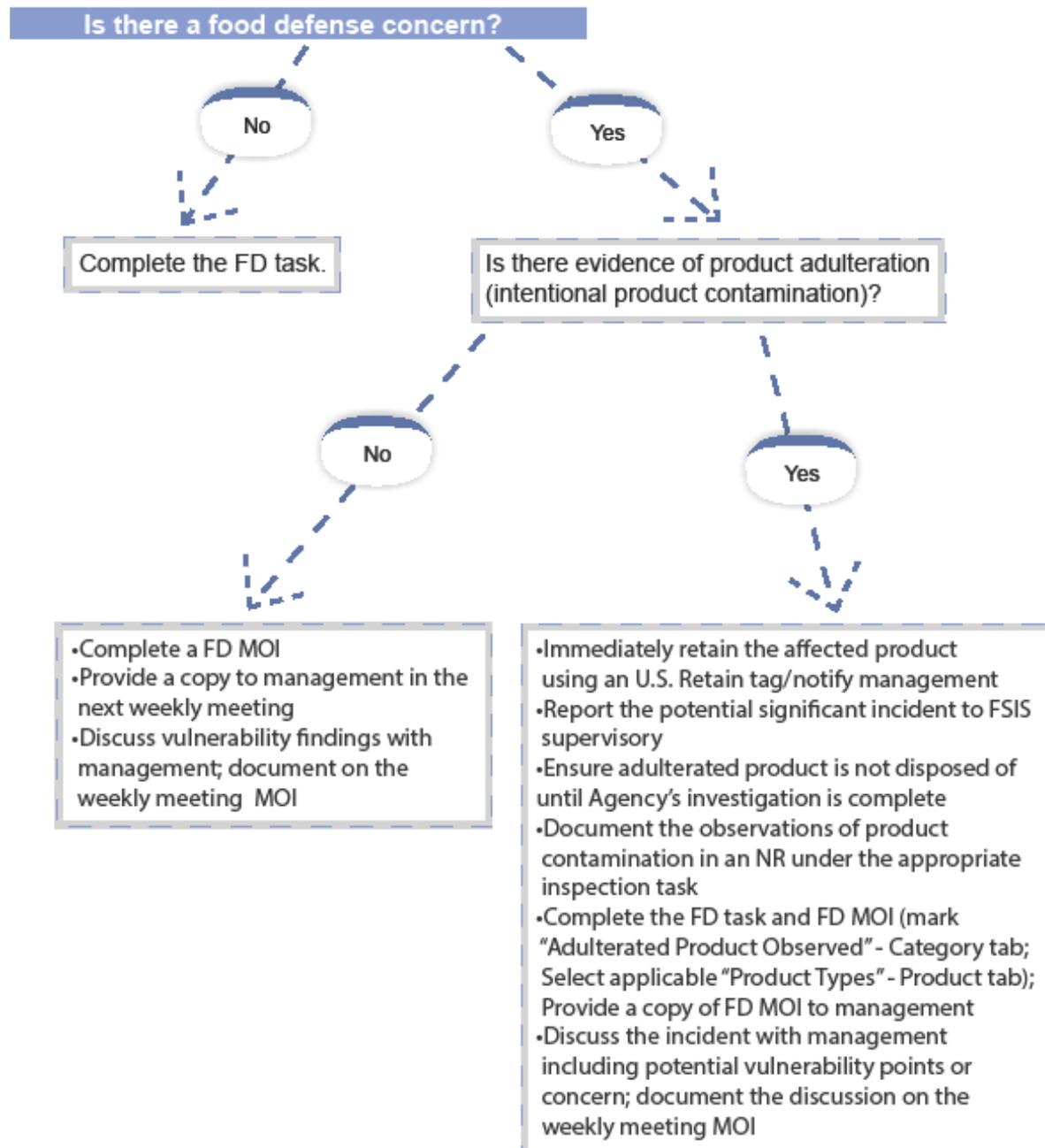
In the case of a NTAS alert identifying an elevated or imminent threat to food or agriculture, the inspector-in-charge (IIC) will receive specific instructions through supervisory channels on other measures to take. If additional Food Defense tasks are necessary, IPP will schedule them as directed task in PHIS. Other measures may include sampling of specific products and deploying inspectors to establishments producing the products to ensure that FSIS has an on-site presence.

If the establishment requests guidance on food defense, IPP are to direct them to the Food Defense web page: (www.fsis.usda.gov/fooddefense) or email: FoodDefense@fsis.usda.gov.

OBSERVING AND DOCUMENTING FOOD DEFENSE VULNERABILITIES

Next is a diagram summarizing the food defense task thought process. Information that is more detailed is to follow. Remember, there is a questionnaire associated with the food defense task that must be completed every time you perform this task.

Food Defense Task Thought Process



When inspection program personnel perform a Food Defense task and do not find a food defense vulnerability or concern, they are to complete the task in PHIS.

IPP may observe food defense vulnerabilities when they are performing the Food Defense task and during other daily inspection activities. IPP should document these vulnerabilities in a food defense memorandum of interview (MOI) after discussing the findings with plant management.

To document a food defense MOI for domestic establishments:

1. Go to the “Inspection Verification” in PHIS and after selecting the establishment, click on “Memorandum of Interview” to open the MOI List page.
2. Click on “Add Food Defense OFO” to open the “Domestic Food Defense MOI” page to access key functions of the MOI.
3. In the “Status” tab, select attendees with left mouse click on attendee’s name. To select more than one attendee, hold “Ctrl” on keyboard while left clicking on each applicable name;
4. In the “Category” tab, choose the appropriate potential vulnerability (No product adulteration observed), the occurrence (1st, 2nd, or 3rd), the establishment size (very small, small, or large), and establishment type (meat, poultry, egg products, or equine);

Note: In case of the 4th occurrence, the establishment express no intention of addressing the situation, IPP are to notify the DO through supervisory channels.

5. In the “Product” tab, leave this table blank.
6. In either the “Processing” or “Storage” tab, identify the vulnerability point or concern. Additional vulnerabilities, other than those related to processing (“Water System”) and storage (“Shipping and Receiving”) activities, are available for selection in these tabs; and
7. Check the “Finalize” box and then click “Save” to complete the Food Defense MOI (FSIS Form 5420-1, see Attachment 2). 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.

When IPP perform a food defense task or other daily inspection activities and find a food defense vulnerability or concern, and there is evidence of product adulteration

(e.g., regulatory non-compliance), IPP will perform a directed HACCP, Sanitation SOP or other appropriate inspection task to record the observed non-compliance citing the applicable regulation. IPP are to:

1. Immediately retain the affected product by attaching a retain tag or detain 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 and follow instructions carefully; IPP should verify and ensure that product **is not disposed of** until being notified, by the Incident Commander through supervisory channels, that the agency's investigation is complete (Directive 5500.4).
3. Add the appropriate inspection verification task (directed HACCP, SSOP or other appropriate inspection task) to the task calendar, document the observed product contamination in an NR, and cite the applicable regulation (SSOP for product contamination or HACCP if product is adulterated).
4. Complete a Food Defense MOI; and

Note: IPP are to mark "Adulterated Product Observed" for Category of Potential Vulnerability under the "Category" tab, and select the applicable product types under the "Product" tab.

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.

SUMMARY

Defending the food supply against intentional contamination is a critical function. IPP, both in and outside of establishments, serve as the Agency's eyes and ears to help identify vulnerabilities that may lead to intentional contamination. IPP are responsible for three activities related to food defense:

- Updating the functional food defense plan status in the PHIS establishment profile and ensuring it is accurate
- Performing food defense tasks
- Submitting a food defense MOI when food defense vulnerability is observed and discuss with establishment management.

Implementation of Food Defense tasks serves to protect the public, which is essential to our mission, and ensures the security of our food, a vital component of homeland security.

Report any suspicious activities in establishments to your district manager through supervisory channels or call the ***FSIS 24-hour emergency hotline*** at ***1-866-395-9761***.

ATTACHMENT 1 - FSIS Food Defense Plan Template

UNITED STATES DEPARTMENT OF AGRICULTURE
FOOD SAFETY AND INSPECTION SERVICE

Food Defense Plan Security Measures for Food Defense

Establishment Name:

Establishment Location (city, state):

FSIS Establishment Number:

By signing here, I acknowledge that this establishment has measures in place in accordance with this document

Print Name: Title:

Signature: Date:

Food Defense Plan Security Measures for Food Defense

Food Defense is having measures in place to reduce the chances of someone intentionally contaminating the food supply in order to kill or hurt people, disrupt our economy, or ruin your business.

PURPOSE

This voluntary plan documents your measures to protect food and food production processes from intentional harm. **Review of this plan and signing the cover sheet will result in a Food Defense Plan for your FSIS-regulated establishment.**

BENEFITS: By having a Food Defense Plan, you will contribute to a safer and more secure food supply. You will also protect public health, your employees, and your livelihood. A functional* food defense plan may also:

- o reduce the risk of unsafe product and economic loss,
- o reduce theft,
- o reduce the need for additional regulation on food defense, and
- o reduce company liability.

INSTRUCTIONS:

1. Review the attached plan.
2. Sign the cover page.
3. On an annual basis, review this plan and document that you did so on the form in **Attachment B**.

This food defense plan is organized in four sections: (1) Outside Security Measures, (2) Inside Security Measures, (3) Personnel Security Measures, and (4) Incident Response Security Measures. **Attachment A** provides a list of tools or additional security measures that an establishment may consider or may already have in place. You may also have other plans that contribute to a food defense plan such as an emergency plan, a recall plan, a security plan, etc. **Attachment B** is a form that can be used to document your annual review of your food defense plan.

*The four elements that make up a *functional* food defense plan:

1. **Develop:** Reviewing and signing this document fulfills this element.
2. **Implement:** Having measures described in this document fulfills this element.
3. **Test:** Periodic monitoring fulfills this element. This can be done using simple measures, such as checking locked doors or making unannounced perimeter checks. Monitoring can be documented using a form, such as **Attachment B**. Not all security measures need to be tested at the same frequency.
4. **Review and Maintain:** Reviewing the plan at least annually, revising the plan as needed, and taking appropriate actions fulfills this element.

Not all measures suggested are appropriate or necessary for every facility.

1. Outside Security Measures

(Examples: door locks, lighting, monitoring loading/unloading)

GOAL: To prevent unauthorized access by people, or entry of unapproved materials to the facility.

This establishment has in place at least one of the following measures for outside security.

1.1 Physical Security

- Plant boundaries are clear and secured to prevent unauthorized entry (for example, fences installed, no trespassing signs posted)
- Entrances are secured (for example, locks and/or alarms installed and operating)
- Plant perimeter is periodically monitored for suspicious activity
- Outside lighting is present to deter unauthorized activities
- Other access points such as windows and vents are secured
- Outside storage on the premises is protected from unauthorized access
- Other:

1.2 Shipping/Receiving Security

- Incoming shipments are examined for potential tampering
- Incoming and outgoing vehicles are examined for suspicious activity
- Loading and unloading activities are scheduled and/or monitored
- Loading dock access is controlled (for example, monitored or locked)
- Incoming shipments are secured with locks or seals
- Outgoing shipments are locked or sealed
- Other:

1.3 Mail Handling Security

- Mail is handled away from food including ingredients and packaged food product
- Employees who handle mail are aware of proper handling of suspicious mail and U.S. Postal Service guidelines
- Other:

Not all measures suggested are appropriate or necessary for every facility.

2. Inside Security Measures
(Examples: signs, observations, restricted access)

GOAL: To protect product from intentional contamination throughout the production process.

This establishment has in place at least one of the following measures for inside security.

2.1 General Inside Security

- Suspicious packages are reported to appropriate personnel
- Restricted areas of the establishment are clearly identified
- Previously unattended materials are checked before use
- Unexpected changes in inventory (product or equipment) are reported to appropriate personnel
- Emergency lighting is in place
- An emergency alert system is identifiable, tested, and reviewed with emergency contacts (for example, police or fire personnel)
- Other: _____

2.2 Slaughter/Processing Area Security

- Access to live animals, ingredients, and packaged product is restricted
- Access to animal handling areas and/or carcass coolers is controlled
- Access to process control equipment such as ovens, mixers is restricted
- Ingredients are examined for possible tampering
- Records ensure traceability for one step backward, one step forward, or both
- Other: _____

2.3 Storage Security

- Access to storage areas is restricted
- Stock rotation (first in, first out) is practiced
- Labels and packaging materials are controlled to prevent theft and misuse
- Periodic examinations for tampering of materials in storage are performed
- Other: _____

Not all measures suggested are appropriate or necessary for every facility.

2. Inside Security Measures

2.4 Ingredients/Water/Ice Security

- Restrict access to storage tanks for potable water and to water reuse systems
- Access to lines that transfer water or ingredients are examined and restricted
- Access to plant ice-making equipment is controlled
- Restricted ingredients (for example, nitrites) are controlled
- Supplier food safety/security information is requested
- Other: _____

2.5 Chemical/Hazardous Material Control Security

- Chemicals/hazardous materials, including pesticides, cleaning or laboratory materials, and sanitizers, are in a restricted area or secured by a lock
- Maintain an up-to-date inventory of hazardous materials and chemicals, and investigate discrepancies
- Potentially hazardous waste (biological or chemical) is controlled and disposed of properly
- Other: _____

2.6 Information Security

- Access to sensitive information such as site plans and processing details is controlled
- Access to computer systems is protected through firewalls and/or passwords
- Other: _____

Not all measures suggested are appropriate or necessary for every facility.

3. Personnel Security Measures

(Examples: check references, use visitor log or sign-in, or check IDs)

GOAL: To ensure that only authorized personnel are in the facility at any time.

This establishment has in place at least one of the following measures for personnel security.

3.1 Employee Security

- A method to recognize or identify employees in the facility is in place
- Background or reference checks are conducted for new hires¹
- Employees have restrictions on what they can bring in or take from the facility (for example, cameras)
- Other:

3.2 Non-employee Security (Example: visitors, contractors, guests, customers, truck drivers)

- A log of non-employees entering the establishment is maintained
- A method to recognize or identify non-employees in the establishment is in place
- Non-employees are chaperoned on-site
- Non-employees are restricted to appropriate areas
- Non-employees have restrictions on what they can bring in or take from the facility
- Other:

3.3 Security Training

- Awareness training on security measures is provided to new employees²
- Refresher awareness training on security measures is offered to employees on a periodic basis²
- Employees are trained to report suspicious activities or unusual observations
- Other:

¹ You can electronically verify the employment eligibility of your new hires at http://www.dhs.gov/files/programs/gc_1185221678150.shtm. E-verify is an internet based system operated by the federal government that is available for employers to use at no charge.

² You can access free food defense awareness training for your employees at <http://www.fda.gov/food/fooddefense/foolseducationalmaterials/default.htm>

Not all measures suggested are appropriate or necessary for every facility.

4. Incident Response Security Measures

(Examples: reference your emergency plan, security plan or other)

GOAL: To respond quickly to a product contamination threat or event using planned measures.

This establishment has in place at least one of the following measures for incident response security.

4.1 Investigating Security Concerns

- Have procedures to ensure that adulterated or potentially harmful products are held
- Customer comments are investigated
- Reporting unusual activities is encouraged
- Information is available to employees on how to respond to phone or other threats
- Employees have the ability to stop activities to minimize a potential food defense incident
- Reported security breaches (for example, alarms, suspicion of tampering) are investigated
- Other:

4.2 Emergency Contact Security

- Plant personnel contact information is kept up to date
- Emergency contact lists are kept up to date
- Other:

4.3 Other Plan Security

- A product recall plan is maintained and periodically reviewed
- Key personnel are trained in product recall/withdraw procedures
- Other:

ATTACHMENT A

**List of Tools or Possible Security Measures
for Food Defense**

This attachment provides a list of tools or additional security measures that an establishment may consider or may already have in place. These are provided to assist establishments in tailoring the plan to meet their specific needs.

1. Outside Security Tools

Physical Security

- Ensure proper lighting to monitor the establishment outdoors at night and early morning.
- Install self-locking doors and/or alarms on emergency exits.
- Ensure the following are secured with locks, seals, or sensors when unattended (after hours/weekends) to prevent unauthorized entry:
 - Outside doors and gates
 - Tanker truck hatches
 - Windows
 - Railcars
 - Roof openings
 - Bulk storage tanks/silos
 - Vent openings
 - Loading ports
 - Trailer (truck) bodies
 - Hose /Pump stations
- Regularly conduct and document security inspections of storage facilities, including temporary storage vehicles.
- Restrict outdoor access to water wells/sources.

Shipping / Receiving Security

- Closely monitor loading and unloading of vehicles transporting raw materials, finished products, or other materials used in food processing.
- Inspect tanker trucks and/or rail cars to detect the presence of any material, solid or liquid, in tanks prior to loading liquid products. Load only when appropriate. Report/record results.
- Control access to loading docks to avoid unverified or unauthorized deliveries.
- Require advance notification from suppliers for all deliveries.
- Immediately investigate suspicious changes in shipping documents.
- Check all deliveries against a roster of scheduled deliveries.
- Hold unscheduled deliveries outside establishment premises pending verification.
- If off-hour delivery is accepted, require prior notice of the delivery and an authorized person to be present to verify and receive the delivery.
- Check less-than-truckload (LTL) or partial load shipments for content and condition.
- Require incoming shipments of raw product, ingredients, and finished products to be sealed with tamper-evident or numbered, documented seals and verify the seals prior to entry. Reject if seals are broken or missing.
- Select transportation companies and suppliers with consideration of security measures that they use.
- Examine returned goods at a separate location for evidence of tampering before salvage or use in rework.
- Maintain records of disposition of returned goods.
- Require drivers or delivery personnel to provide identification, preferably with a photo ID. Record names.
- Minimize the time a truck is unlocked during loading or delivery.

List of Tools or Possible Security Measures for Food Defense

Not all measures suggested are appropriate or necessary for every facility.

2. Inside Security Tools

General Inside Security

- Install and monitor security cameras.
- Increase visibility within the establishment (for example, improve lighting, openness, increase supervision, add cameras).
- Regularly take inventory of keys to secured/sensitive areas of the establishment.
- Restrict access to controls (by locked door/gate or limiting access to designated employees) for the following systems:
 - Heating, ventilation, and air conditioning (HVAC)
 - Propane, natural gas, water, electricity
 - Disinfection systems
 - Clean-in place (CIP) systems or other centralized chemical systems

Slaughter / Processing Area Security

- Maintain records to allow efficient trace backward or forward of materials and finished product.
- Reduce the time an area is left unmonitored.
- Reduce access to product containers or processing equipment.
- Do not allow unnecessary personal items within the production area.

Storage Security

- Maintain an access log for product and ingredient storage areas.
- Regularly check the inventory of finished products for unexplained additions and withdrawals from existing stock.
- Restrict access to external storage facilities to designated employees only.

Ingredients / Water / Ice Security

- Examine packages of ingredients before use for evidence of tampering.
- Restrict access to product, ingredient, and packaging storage areas to designated employees only (by locked door/gate).
- Water is from a municipally controlled source.
- Inspect water lines for possible tampering (perform visual inspection for integrity of infrastructure, proper connections).
- Make arrangements with local health officials to ensure immediate notification to the establishment if the potability of the public water supply is compromised.

Chemical / Hazardous Material Control Security

- Restrict access to the in-plant laboratory.
- Have procedures in place to control receipt of samples.
- Have a procedure in place to receive, securely store, and dispose of reagents.

Information Security

- Track customer complaints/comments for trends.
- Keep details of food defense procedures confidential as necessary.
- Have up-to-date establishment layout/blueprints for local law enforcement, including the fire department if needed.

List of Tools or Possible Security Measures for Food Defense

Not all measures suggested are appropriate or necessary for every facility.

3. Personnel Security Tools

- Authorize appropriate employees to stop a process for significant concerns.
- Control access by employees and non-employees entering the establishment during working and non-working hours (use coded doors, receptionist on duty, swipe cards).
- Restrict temporary employees and non-employees to areas relevant to their work.
- Implement system to identify personnel with their specific functions, assignments or departments (for example, corresponding colored uniforms or hair covers).
- Prohibit employees from removing company-provided uniforms or protective gear from the premises.
- Maintain an updated shift roster for each shift.

4. Incident Response Tools

- Establish evacuation procedures and include in food defense plan.
- Establish procedures for responding to threats as well as actual product contamination events.
- Pre-establish communication with local, state, and federal incident response personnel for a more efficient response.

ATTACHMENT B - Food Defense Plan Review

Complete this form to document your annual review of this Food Defense Plan.

Not all measures are required or need to be reviewed each time this form is completed.

Date of Annual Review	Person Who Conducted Annual Review (Name and Title)	Was the Food Defense Plan tested?*(Yes / No)
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> Yes <input type="checkbox"/> No

*Testing can be done using simple measures, such as checking locked doors or making unannounced perimeter checks.

NOTE: Make as many copies of this page as necessary.

Attachment 2 - FSIS Form 5420-1

U.S. Department of Agriculture Food Safety and Inspection Service FOOD DEFENSE MEMORANDUM OF INTERVIEW SENSITIVE SECURITY INFORMATION Distribute One Copy To: Plant Management, District Analyst & IF-OFDER mailbox		1. ESTABLISHMENT NUMBER: M45711	
		2. ESTABLISHMENT NAME: Groveton Meats88, Inc.	
3a. CATEGORY OF POTENTIAL VULNERABILITY: <input checked="" type="checkbox"/> No product adulteration observed <input type="checkbox"/> Adulterated product observed		3b. OCCURENCE: <input checked="" type="checkbox"/> 1st <input type="checkbox"/> 2nd <input type="checkbox"/> 3rd	
		4. SIZE OF PLANT: <input type="checkbox"/> Very Small <input type="checkbox"/> Small <input checked="" type="checkbox"/> Large	
5. PRODUCT TYPE: <input type="checkbox"/> Raw - Non Intact <input checked="" type="checkbox"/> Raw - Intact <input type="checkbox"/> Thermally Processed/Commercially Sterile <input type="checkbox"/> Not Heat Treated - Shelf Stable <input type="checkbox"/> Heat Treated - Shelf Stable <input type="checkbox"/> Fully Cooked - Not Shelf Stable <input type="checkbox"/> Heat Treated - Not Fully Cooked - Not Shelf Stable <input type="checkbox"/> Product with Secondary Inhibitors - Not Shelf Stable		6. PLANT TYPE: <input type="checkbox"/> Meat <input checked="" type="checkbox"/> Poultry <input type="checkbox"/> Egg <input type="checkbox"/> Equine	
7. WATER SYSTEMS: <input checked="" type="checkbox"/> Unrestricted Access to Outside Well <input checked="" type="checkbox"/> Unrestricted Access to In-Plant Water Systems, Water Storage Tanks or Ice Machines on Premises			
8. PROCESSING AREA/MANUFACTURING: <input checked="" type="checkbox"/> Unrestricted Access to Sensitive Processing Areas by Unauthorized Individuals (including employees or maintenance workers) <input type="checkbox"/> Equipment Calibration Incorrect <input type="checkbox"/> Evidence of Possible Intentional Contamination Observed			
9. STORAGE AREAS: <input type="checkbox"/> Evidence of Possible Tampering on Stored Product <input type="checkbox"/> Unrestricted Access to Dry Ingredients <input type="checkbox"/> Unrestricted Access to Raw Product Ingredients <input type="checkbox"/> Unrestricted Access to Finished Product <input type="checkbox"/> Unrestricted Access to/use of Hazardous Chemicals			
10. SHIPPING AND RECEIVING: <input type="checkbox"/> Unrestricted Access to Loading Docks <input type="checkbox"/> No Verification of Incoming Shipment of Raw Materials			
11. PLANT MANAGEMENT RESPONSE:			
12. NAME OF INSPECTOR: Robert Barclay88		13. DATE: 5/13/2019	
FSIS FORM 5420-1 (09/08/2006)			