

## Food Defense

### OBJECTIVES

The objectives for this module are to:

1. Describe the risk that intentional contamination presents to FSIS-regulated establishments.
2. Define key food defense terms.
3. Identify food defense vulnerabilities and associated mitigation strategies.
4. Describe the purpose of the food defense task with respect to identifying potential food defense vulnerabilities in FSIS-regulated establishments.
5. Identify the steps taken to encourage an establishment to implement food defense practices to protect their product from intentional contamination.

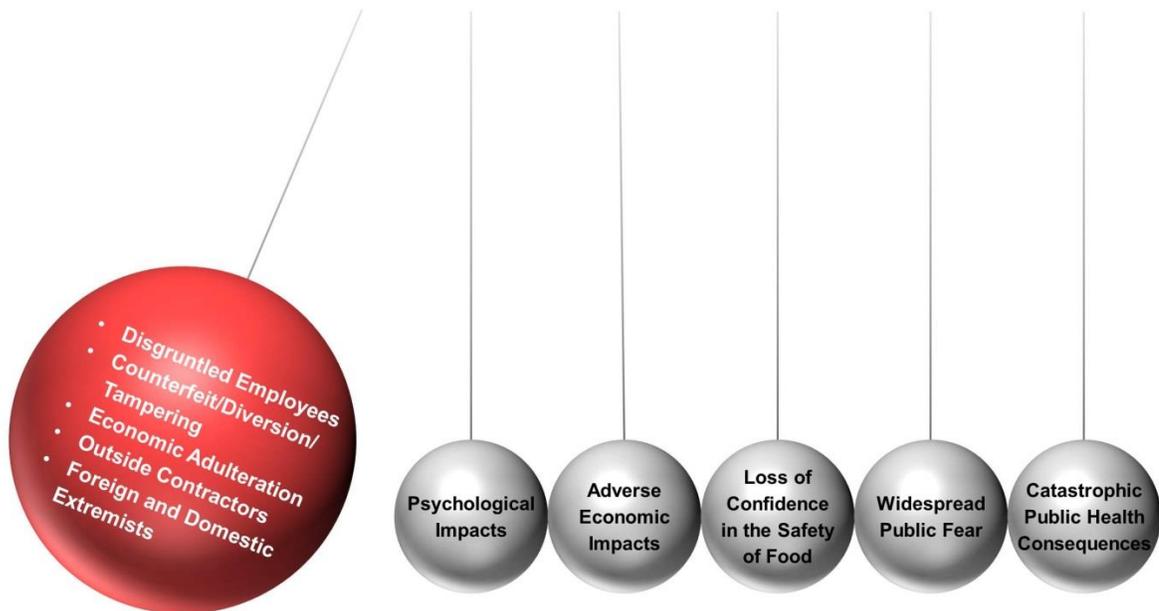
### REFERENCES

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. 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 [Food Defense Assessment Staff](#) (FDAS) within FSIS' Office of Data Integration and Food Protection is responsible for managing all food defense activities for the Agency. FDAS 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 (refer to Attachment 3 – Additional Information on Food Defense). The primary functions of the FDAS include:

- Collaborating with Federal, state, local, and tribal governments, industry, and academic partners to promote food defense;
- Developing and sharing guidance for developing and maintaining food defense practices, including functional food defense plans;
- Conducting vulnerability assessments;
- Identifying and implementing countermeasures and mitigation strategies;
- Conducting analysis of food defense surveillance data;
- Maintaining close relationships with the intelligence and law enforcement communities to educate collectors and analysts on food defense to better inform their work and enhance the exchange of information; and
- Working with the scientific community on food defense research initiatives, integrated project teams, and risk assessment workgroups.

The Food Defense Assessment Staff is available at any time to answer questions related to food defense and can be reached via email at [FoodDefense@fsis.usda.gov](mailto:FoodDefense@fsis.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. While the United States has a well-functioning food safety infrastructure to protect the public against the unintentional contamination of food, *food defense* encompasses a broader range of considerations.

**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.

**Agroterrorism** – terrorist acts intended to disrupt or damage a country's agriculture for the purpose of causing injury or death to civilian populations or disrupting social, economic, or political stability (for more information, see Attachment 4 – Bioterrorism Overview). Within FSIS, agroterrorism is further focused on how terrorism relates to meat, poultry and egg products.

**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 MITIGATION STRATEGIES

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. It should be noted that **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 (FDP).

A functional FDP 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 FDP is functional when all four of the following criteria are met:

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:** If the establishment were not implementing elements of its FDP, then FSIS would not consider the establishment to have a functional FDP.

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. Even though functional FDPs are voluntary, FSIS considers such plans to be an important tool

that can reduce the risk of intentional adulteration of food products. Consequently, an establishment does not have to provide IPP access to its FDP 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. An example of FSIS' food defense plan template is provided in Attachment 2.

IPP are responsible for updating and maintaining the functional FDP 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 FDP. This status is to 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 FDP status.

## **NATIONAL TERRORISM ADVISORY SYSTEM**

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

NTAS consists of two types of advisories:

- **Bulletins** – Communicate current developments or general trends regarding threats of terrorism and provide the Secretary of DHS with greater flexibility to make available the information to stakeholders and members of the public in a timely manner. In the bulletin, it summarizes the issue and why is important for public awareness.
- **Alerts** – When 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.

In some cases, alerts are sent directly to law enforcement or affected areas of the private sector. In others, alerts are issued more broadly to the American people through official and media channels, including a designated [DHS - NTAS](#) webpage or social media tools, such as Facebook and Twitter. Additionally, NTAS has a “sunset provision”, meaning that individual threat alerts are issued with a specified end date. Alerts may be extended if new information becomes available or if the threat evolves significantly.

## **FSIS DIRECTIVES**

Now, let us talk more specifically about your duties related to food defense. Your duties are covered in the 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

When reviewing any of these Directives, make sure that you have the most recently issued version by downloading the particular Directive from the [FSIS](#) website or PHIS – Home Page – My Dashboard tab. These may be modified frequently to reflect new threat information gained through intelligence gathering activities conducted worldwide. Therefore, it is imperative that you review these directives following notification of any modifications or updates.

FSIS conducts surveillance activities throughout the food production process. The food production process consists of a series of processes along the farm to table chain. The order of these processes is:

- Production – is the growth of food products and shipment of the products to the slaughter or processing facilities. The shipping portion of this process also accounts for imported products.
- Processing – is the slaughter and processing steps of the chain.
- Distribution – is the movement of the processed product into commerce.
- Retail/Consumption – the final step when the product reaches the retail service industry (institutional facilities and/or grocers).

The FSIS in-plant inspection team's major area of responsibility falls within the processing part of the system. 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 Food Defense (FD) task that Inspection Program Personnel (IPP) are to perform in the Public Health Information System (PHIS) and the frequency with which this task is to be performed. 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 Office of Data Integration and Food Protection (ODIFP) Assistant Administrator (AA) 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 ODIFP AA or designee is to inform the FSIS Administrator and FSIS Management Council;
3. The ODIFP AA or designee is to determine the appropriate distribution of the threat information and coordinate with OFO, Office of Investigation, Enforcement and Audit (OIEA), the Office of Public Affairs and Consumer

Education (OPACE), and the 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](#).

Supervisory personnel are to ensure that any notifications distributed to field employees pursuant to this directive 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 [FSIS Directive 5010.1, Food Safety Related Topics During Weekly Meetings](#)).

ODIFP is to notify the FSIS Administrator and the FSIS Management Council of any changes in threat information, to include when the period of concern has expired. ODIFP is to coordinate with OFO, OIEA, OPACE, 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.

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.

When the Federal government receives information about a specific or credible terrorist threat to food or agriculture, additional FD tasks may be necessary, and additional actions may be needed to reduce the threat of intentional adulteration of food products. Given what is required in responding to a credible threat of a terrorist attack, 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 FD 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 in meat and poultry establishments perform the FD task to identify vulnerabilities within establishments that may lead to intentional contamination of FSIS-regulated products. 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. Examples may include, but are not limited to, unrestricted access to the water system or to a processing room, or uncontrolled access to a restricted ingredient area. There are resources that the IPP can use, as well as industry, as an aid to assess vulnerabilities while performing the FD task. These resources can be found on FSIS' food defense webpage ([www.fsis.usda.gov/fooddefense](http://www.fsis.usda.gov/fooddefense)), 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.

Task questions are provided in the table in Section VI of the directive. Prior to completing the questionnaire, IPP should discuss food defense activities with management during a weekly meeting to learn more about the establishment's FD practices. This will allow them to more 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 FD vulnerability exists and mitigation strategies to address to identified vulnerabilities and weaknesses in the establishment. 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 if any, that he or she is to take based on the information received about the specific threat to a product or process. If additional FD tasks are necessary, IPP will schedule them as directed task in PHIS following instructions as per Directive 13,000.1. Other measures may include sampling of specific products, to protect public health, and deploy IPP to establishments producing the products to ensure that FSIS has an on-site presence during any type of operational activity.

If the establishment requests guidance or additional information on food defense, including how to develop a functional FDP, IPP are to direct the establishment to the Food Defense web page ([www.fsis.usda.gov/fooddefense](http://www.fsis.usda.gov/fooddefense)) or email [FoodDefense@fsis.usda.gov](mailto:FoodDefense@fsis.usda.gov).

## **OBSERVING AND DOCUMENTING FOOD DEFENSE VULNERABILITIES**

IPP may observe food defense vulnerabilities when they are performing the FD task and during other daily inspection activities. IPP can 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 4<sup>th</sup> 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 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.

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 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

**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.

## **Food Defense Tasks in Facilities Paying Fees for Inspection Service**

In accordance to 9 CFR Parts 350, 351, 352, and 354, no routine FD task will be assigned. FSIS encourages these facilities to develop a functional FDP, and if management request guidance or additional information on food defense, including on how to develop a functional FDP, IPP are to direct establishment to the Food Defense webpage ([www.fsis.usda.gov/fooddefense](http://www.fsis.usda.gov/fooddefense)).

### **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 discussed with establishment management.

Implementation of FD 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 Form 5420-1

U.S. Department of Agriculture Food Safety and Inspection Service <b>FOOD DEFENSE MEMORANDUM OF INTERVIEW</b> <b>SENSITIVE SECURITY INFORMATION</b> Distribute One Copy To: Plant Management, District Analyst & IF-OFDER mailbox		1. ESTABLISHMENT NUMBER: P0000	
		2. ESTABLISHMENT NAME: XXXX	
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 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 type="checkbox"/> Verified Whether Facility Restricts Access to Outside Well <input type="checkbox"/> Verified Whether Facility Restricts Access to In-Plant Water Systems, Water Storage Tanks or Ice Machines on Premises			
8. PROCESSING AREA/MANUFACTURING: <input type="checkbox"/> Verified Whether Facility Restricts Access to Sensitive Processing Areas by Unauthorized Individuals (including employees or maintenance workers) <input type="checkbox"/> Verified Whether Equipment Calibration is Correct <input type="checkbox"/> looked for Evidence of Possible Intentional Contamination			
9. STORAGE AREAS: <input type="checkbox"/> Looked for Evidence of Possible Tampering with Stored Product <input checked="" type="checkbox"/> Verified Whether Facility Restricts Access to Dry Ingredients <input checked="" type="checkbox"/> Verified Whether Facility Restricts Access to Raw Product Ingredients <input type="checkbox"/> Verified Whether Facility Restricts Access to Finished Product <input type="checkbox"/> Verified Whether Facility Restricts Access to and use of Hazardous Chemicals			
10. SHIPPING AND RECEIVING: <input type="checkbox"/> Verified Whether Facility Restricts Access to Loading Docks <input type="checkbox"/> Verified Whether Facility Verifies Incoming Shipment of Raw Materials			
11. PLANT MANAGEMENT RESPONSE:			
12. NAME OF INSPECTOR: XXX		13. DATE X/XX/XXXX	
FSIS FORM 5420-1 (09/08/2006)			

## ATTACHMENT 2: 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 hires<sup>1</sup>
- 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 employees<sup>2</sup>
- Refresher awareness training on security measures is offered to employees on a periodic basis<sup>2</sup>
- Employees are trained to report suspicious activities or unusual observations
- Other: \_\_\_\_\_

---

<sup>1</sup> You can electronically verify the employment eligibility of your new hires at [http://www.dhs.gov/files/programs/gc\\_1185221678150.shtm](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.

<sup>2</sup> You can access free food defense awareness training for your employees at <http://www.fda.gov/food/fooddefense/toolseducationalmaterials/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="checkbox"/> Yes <input type="checkbox"/> No
		<input type="checkbox"/> Yes <input type="checkbox"/> No
		<input type="checkbox"/> Yes <input type="checkbox"/> No
		<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 3: Additional Information on Food Defense**

The events of September 11, 2001, brought the issue of the vulnerability of our food supply to the forefront. Tommy Thompson, a former Secretary of the Department of Health and Human Services (DHHS), has stated, “For the life of me, I cannot understand why the terrorists have not attacked our food supply because it is so easy to do.” Bill Frist, a physician, former Senator, and one of the original sponsors of the Bioterrorism Preparedness Act signed into law in 2002, has stated that “...as we consider bioterrorism, we are most vulnerable in our food supply.” We in FSIS must make consideration of the “unusual” as part of how we routinely conduct business by remaining ever vigilant of possible attacks on the food supply and wary of situations that appear out of the ordinary. We must accept the fact that an attack on our food supply is plausible.

FSIS has identified food defense activities that the Agency is doing to meet the challenges of food defense. In addition, FSIS has taken steps to promote the adoption of preventive strategies by private industries to ensure the security of meat, poultry, and egg products. Following is an overview of the activities FSIS has taken to ensure that meat, poultry, and egg products are protected from intentional adulteration.

### **EXAMPLES OF ATTACKS ON THE FOOD SUPPLY**

History has shown that terrorists can, and will, use food as a weapon. A review of a few noteworthy intentional food borne disease outbreaks provides insight into:

- The kinds of foods and the points in their production where intentional contamination could have catastrophic consequences,
- The potential magnitude of the public health impact of a carefully planned intentional attack on the food supply, and
- Some of the types of individuals and their motivations for intentionally attacking the food supply.

Following is a description of some historical events that highlight the need for concern and action regarding protecting the food supply against intentional contamination.

- In 1972, members of a U.S. fascist group called Order of the Rising Sun were found in possession of 30-40 kilograms of typhoid bacteria cultures, with which they planned to contaminate water supplies in Chicago, St. Louis, and other Midwestern cities.
- In 1984, two members of an Oregon cult headed by Bhagwan Shree Rajneesh cultivated *Salmonella* (food poisoning) bacteria, and used it to

contaminate restaurant salad bars in an attempt to affect the outcome of a local election. Although some 751 people became ill, and 45 were hospitalized; there were no fatalities.

- In early March 1989, someone created a scare that grapes from Chile imported into the USA would be contaminated with cyanide. On March 11, the United States Food and Drug Administration (FDA) spotted three suspicious-looking grapes on the docks in Philadelphia, in a shipment that had just arrived from Chile. Two of the grapes had puncture marks. They were tested and found to contain low levels of cyanide. The FDA impounded 2 million crates of fruit at ports across the country and warned consumers not to eat any fruit from Chile, which included most of the peaches, blueberries, blackberries, melons, green apples, pears, and plums that were on the market at the time.
- October 1996, a former laboratory employee at the St. Paul Medical Center in Dallas, pleaded guilty to engaging in her own personal act of food-borne terrorism by intentionally contaminating pastries. She had access to the highly toxic bacteria, *Shigella dysenteriae*, stored in the laboratory; she contaminated the pastries and left them in an employee break room, and she sent a bogus e-mail message from her supervisor's computer notifying laboratory employees of the free snacks in the break room. Her activities were discovered when she tried to alter hospital records to cover her tracks.
- In 1996, police received an anonymous call from a worker at a rendering establishment in Wisconsin. The caller said liquid fat from the establishment had been contaminated. It was determined that chlordane was the contaminant, an organochlorine pesticide that is environmentally stable, accumulates in the fat of animals, and is considered a food adulterant at very low levels (0.3 ppm in animal fat). This fat found its way to feed manufacturers and eventually onto nearly 4,000 farms in Wisconsin, Minnesota, Michigan and Illinois. Within two days, all major customers were notified and the feed was replaced. Luckily, milk samples taken from some of the dairy herds that had eaten the affected feed were negative or contained levels well below those that which poses a health hazard to humans. Total costs for disposing of the contaminated feed (4,000 tons) and fat (500,000 pounds) was almost \$4 million; however, as numerous state and federal agencies became involved in dealing with this issue, the final price tag was likely much higher.
- On January 3, 2003, the Michigan Department of Agriculture's Food and Dairy Division and the U.S. Department of Agriculture were notified by a supermarket of a planned recall of approximately 1,700 pounds of ground beef because customers had complained of illness after eating the product. The contaminant in the ground beef returned by customers with

reported illness was identified as nicotine from nicotine-based pesticide used by the supermarket. An employee of the supermarket was arrested and charged with deliberately poisoning the ground beef at the supermarket.

## VULNERABILITY ASSESSMENTS

Being aware of what terrorists do, how they do it, and when and where they do it can help us be more effective in identifying and preventing their activities. How can a terrorist organization gain technical capability? Can they recruit American food system workers? Can they gain knowledge by talking with food system workers using what appear to be simple and innocent questions about their jobs while sitting at a baseball game or standing in line at a grocery store? Food system workers are a prime information target; and that includes you. What must a terrorist have to carry out an attack? A terrorist must have the following to conduct agroterrorism activities:

- Have access to the food for a sufficient amount of time to tamper with it;
- Be technically capable of introducing a contaminant;
- Be able to perform the operation without discovery; and
- Be competent enough to avoid detection of the adulterated product down stream in the production's distribution life cycle.

FSIS conducts vulnerability assessments to better prevent and protect against an intentional attack on its regulated products. Based on the assessments, FSIS develops countermeasures to protect the food supply as directed by [Homeland Security Presidential Directive-9](#) (HSPD-9). Additionally, these assessments help to identify research gaps and strengthen communication and collaboration between government and industry partners.

From these assessments, certain activity types (e.g., bulk liquid receiving and loading; liquid storage and handling; secondary ingredient handling; and mixing and similar activities) and characteristics (e.g., short shelf life, large batch size, uniform mixing, accessibility to the product) were identified that present unique vulnerability to intentional contamination. These activity types and characteristics may occur at multiple process and distribution steps within the supply chain.

To further elaborate, large batch size places a food product at high risk because it facilitates the contamination of a large quantity of product all at the same time. In turn, a large number of individuals may consume the contaminated product. The larger the number of consumers, there will be a greater potential for a larger number of deaths or illnesses. For instance, contamination of a 5,000-gallon commercial kettle could negatively affect a much larger number of individuals than contamination of a 5-gallon food service pot. Uniform mixing places a

product at high risk for contamination because adding agents before or during mixing steps results in contamination of all of the servings in a batch, improving the efficiency of an attack. Short shelf life places a food product at risk because these products may be consumed before public health officials are able to identify the cause of illness and to take action to prevent further illnesses. Ease of access increases a products risk for adulteration because carrying out an act requires access to the product or its raw materials. The more accessible a site the more likely it will be a target.

Vulnerability assessments also help to identify food defense countermeasures and mitigation strategies aimed at preventing or reducing the impact of an intentional attack on the food supply. Mitigation strategies are *risk-based, reasonably appropriate measures that a person knowledgeable about food defense would employ to significantly minimize or prevent significant vulnerabilities identified at actionable process steps, and that are consistent with the current scientific understanding of food defense at the time of the analysis.* Mitigation strategies can apply to multiple commodities or facility types, or they can be customized for a specific commodity or facility. Once vulnerabilities and corresponding mitigation strategies have been identified, they can be used to develop a food defense plan.

Vulnerability assessments have also shed some light on types of individuals that might be motivated to adulterate food products:

- Attacks from internal sources are possibly the most difficult to prevent because they typically know what procedures are followed in the establishment and often know how to bypass many security controls that would detect or delay an external intruder. Disgruntled insiders are generally motivated by their own emotions and self-interests. They may be mentally unstable, operating impulsively with minimal planning. This may be the most difficult group to stop because they may have legitimate access to the product.
- Criminals who are sophisticated may possess relatively refined skills and tools and are generally interested in high-value targets. Unsophisticated criminals have more crude skills and tools and typically have no formal organization. They are generally interested in targets that pose a low risk of detection.
- Protestors are usually politically or issue-oriented. They generally act out of frustration, discontent, or anger. They are primarily interested in publicity for their cause, and generally do not intend to injure people, but may be superficially destructive. They are usually unsophisticated in their tactics and planning. However, some protest groups have adapted tactics similar to terrorists. In this way, they may be moderately sophisticated and moderately destructive. In fact, they may target individuals for harm.

- Subversives, also known as saboteurs, assassins, guerrillas, or commandos are sophisticated, highly skilled, and capable of meticulous planning. Subversives typically operate in small groups with objectives including death, destruction, and targeting personnel, equipment, and operations.
- Terrorists are usually politically or ideologically oriented. They typically work in small, well-organized groups. They are typically well funded, sophisticated, and capable of efficient planning. Terrorists may use other types of aggressors to accomplish their goals. Their objectives include death, destruction, theft, and publicity.

## **FSIS FOOD DEFENSE STRATEGY**

The nation's awareness of terrorism has been heightened and there is an intense focus on ensuring the protection of the nation's critical infrastructures. Section 332 of the Public Health Security and Bioterrorism Act of 2002 established that the Secretary of Agriculture might utilize existing authorities granted by the FMIA, PPIA, and EPIA to give high priority to enhancing and expanding the capacity of FSIS to conduct activities related to food defense. Homeland Security Presidential Directive (HSPD) 7 established a national policy for Federal departments and agencies to identify and prioritize critical infrastructures and key resources and to protect them from terrorist attacks. HSPD-9 established a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies. HSPD-9 outlines roles and responsibilities for USDA, DHHS, and the Environmental Protection Agency (EPA) in planning for, preventing, and responding to such emergencies.

An example of applying the expectations of Section 332 of the Bioterrorism Act occurred at the beginning of the war in Iraq when the federal government was on heightened alert. We had real concern that our nation would be the subject of a terrorist attack in retaliation for the war. "Liberty Shield" was the code word for the government's heightened alert reactions. During that time, FSIS put into effect a number of "prevention" measures that would be the basis of our future actions and response to changes in threat conditions. For example, Inspectors-In-Charge (IICs) initiated new security-based inspection measures as part of their verification activities. Import inspectors also increased security oversight. Laboratory sampling was increased so that 50% of all samples included analysis for a threat agent, and the Consumer Complaint Monitoring System (CCMS) increased its coverage. FSIS epidemiologists enhanced their surveillance efforts for human illnesses, looking for possible links to unusual disease signs.

During Operation Liberty Shield, instructions were provided to field Public Health Veterinarians and inspectors to replace certain non-food safety inspection

procedures with targeted inspection and sampling for a dozen or so biological, chemical, or radiological agents. Since then, FSIS continues to randomly test for these agents on an ongoing basis to maintain surveillance and monitoring for terrorism.

The example of Operation Liberty Shield points to the fact that efforts to improve the security of the food supply in particular must focus on prevention, early detection, containment of contaminated product, and mitigation and remediation of any problems that do occur. These efforts are not without significant challenges, including the following:

- There is no strong statutory authority to mandate security measures.
- Many points along the farm-to-table continuum could be targets of agricultural bioterrorism in general and agroterrorism specifically.

FSIS created the Office of Data Integration and Food Protection (ODIFP) in 2002 to coordinate the Agency's food defense activities. The mission of ODIFP is to develop and coordinate all FSIS activities to prevent, prepare for, respond to, and recover from non-routine emergencies resulting from intentional and non-intentional contamination affecting meat, poultry, and egg products. ODIFP serves as the agency's central office for homeland security issues and ensures coordination of its activities with the USDA Homeland Security Office, the White House, the Department of Homeland Security (DHS), the Food and Drug Administration (FDA), and other Federal and State government agencies with food-related responsibilities, and industry. ODIFP has a comprehensive strategy for dealing with food defense challenges including:

- Vulnerability assessments
- Emergency preparedness and continuity of operations (COOP) planning
- Surveillance and data analysis, including predictive analytics
- Outreach and training
- Collaboration
- Promoting food defense research

In response to President Bush's issuance of the Homeland Security Presidential Directive that called for establishing a single, comprehensive national incident management system FSIS along with other agencies, have adopted the Incident Command System (ICS). ICS was designed in the early '70s. It is a standardized on-scene incident management concept that allows responders from multiple agencies to adopt a flexible, integrated organizational structure to cope with an emergency. The organizational structure is specific to the ICS concept, and does not necessarily align with the organizational structure of any of the responding agencies. Thus, the Incident Commander, and those he/she commands, may not

all be from one agency or the head of any particular agency. ICS utilizes the skills of those most qualified to take command of the particular situation until the emergency has been abated. In order to ensure a seamless FSIS response, certain FSIS employees (DO and above) have been required to complete the ICS training. ICS courses are available through AgLearn. To date, FSIS has entered into cooperative agreements with the Department of Homeland Security, the Department of Health and Human Services, Food and Drug Administration, and the National Association of State Departments of Agriculture's (NASDA) to ensure that a prevention and response mechanism between federal and state agencies could be enacted under the ICS system.

ODIFP developed the FSIS supplement to the USDA's Continuity of Operations Plan (COOP). A COOP identifies critical essential functions, succession and delegation of authority, and essential documents, and then attempts to define how the Agency will maintain mission critical functions and capabilities, communications, and security under non-routine circumstances. Examples of non-routine circumstances might be a large-scale attack on the country, a natural disaster, or an avian influenza pandemic (more examples given below). If there were an attack on headquarters in Washington, DC, for example, the headquarters COOP enables other parts of the Agency to take over the functions of headquarters at other locations. Regarding an avian influenza pandemic, ODIFP has done extensive planning to ensure the safety and health of FSIS employees and the delivery of essential functions. More generally, FSIS has identified and developed response plans to help protect employees from exposure to bioterrorism agents, including procurement of analytical detection equipment.

FSIS has established the Emergency Management Committee (EMC), a standing committee that may be activated at any time to address and manage the Agency's response to a significant incident involving the adulteration of FSIS-regulated product or to manage a significant event or potential public health issue that requires coordination and sharing of resources among program areas. The National Biosurveillance Information System (NBIS) tracks and manage significant incidents. A significant incident presents a grave or potentially grave threat to public health involving FSIS-regulated product. Examples of significant incidents include the following:

- Widespread, or life-threatening, human illnesses potentially implicating FSIS-regulated product;
- Deliberate contamination of FSIS-regulated product;
- Threat alerts that there is an "imminent threat" or "elevated threat" specific to the food and agricultural sector;
- Widespread animal disease with potentially significant public health implications for FSIS-regulated product;
- Ineligible foreign product in the United States

- High risk products in the US as identified by Customs and Border Protection;
- Suspicious activities observed by program personnel while performing their normal duties.
- Natural disasters (e.g., hurricanes, tornadoes, earthquakes);
- Terrorist attacks on the nation's critical infrastructures; and
- Other Incidents of National Significance (INS) that result in the activation of the Emergency Support Function -11 (ESF-11), which are described in the Agriculture and Natural Resources Annex to the National Response Plan

From time-to-time, the EMC may need to form an Incident Investigation Team (IIT) to investigate and provide information regarding a particular emergency incident. These IIT reviews typically would be in response to an illness or outbreak in which a meat, poultry, or egg product produced by an establishment has been implicated; significant or repetitive contamination or adulteration incidents; or repetitive microbiological sampling failures as a result of either the Agency or establishment testing (e.g., *Escherichia coli* O157:H7, *Listeria monocytogenes*, or *Salmonella*). These teams would utilize specially developed protocols and methodologies to gather the necessary information.

FSIS also has a number of surveillance activities underway. For example, FSIS continues to enhance the Consumer Complaint Monitoring System (CCMS). The CCMS is a surveillance system that monitors and tracks food-related consumer complaints. It is a potentially powerful tool in serving as a sentinel system for terrorist attacks on the food supply. FSIS also participates in FoodNet, and maintains a regulatory sampling database. FSIS has a liaison at the CDC in Atlanta. Some of these activities were established for food safety reasons, but can be used for food security as well.

The Office of Public Health Science (OPHS) Epidemiology Officers offer another source for surveillance. The Epidemiology Officers with District Offices oversight have taken on an important surveillance and response role for food defense, as part of their responsibilities. They conduct regular surveillance activities, and have specialized roles to respond to food defense emergencies.

Enhanced laboratory capability was established with The Food Emergency Response Network (FERN). FERN was established in February of 2005. Working with FDA, FERN's mission is to expand and manage an existing group of more than 90 federal, state, and local laboratories with the capability to detect and identify biological, chemical, and radiological agents. FERN is located alongside the FSIS Eastern Lab. In its own laboratories, FSIS has conducted security assessments, improved security, obtained screening equipment and methods for threat agents, and developed protocols that ensure proper chain of custody and other controls on all samples taken at official establishments. FSIS continues to develop a Biosafety Level 3 laboratory to test for threat agents in food products

(such as *Mycobacterium tuberculosis*, St. Louis encephalitis, and *Bacillus anthracis*).

FSIS workforce training in food defense has primarily focused on prevention of terrorist activities, rather than responding to an event. Currently available training materials include FSIS Directive 5420.1 that provides instruction on policy for field personnel. IPP trainees need to read FSIS Directive 5420.1 to learn how to perform the food defense task. An online course on food defense awareness developed cooperatively by the FDA and USDA is available at <http://www.fda.gov/ora/training/orau/FoodSecurity/default.htm>. In addition, FDA has developed several food defense-training courses, which can be found at <https://www.fda.gov/Food/FoodDefense/ToolsEducationalMaterials/default.htm>.

For those interested in Incident Command System (ICS) training, which is currently not mandatory for in-plant inspection personnel, AgLearn offers several courses on ICS. AgLearn can be accessed through <http://www.aglearn.usda.gov>. USDA eAuthentication credentials are required to login.

## Industry Outreach

There currently are no regulatory requirements specific to food defense; however, FSIS encourages the private industry to develop a functional food defense plan and implement food defense practices to minimize their risk of an agroterrorism incident. In an effort to help private industry minimize their risk, FSIS has developed publications and tools to promote food defense activities by all food businesses. These publications encourage industry to take steps to ensure the security of their operations, and have been designed to be especially helpful to small and very small establishments that may not have the resources of larger corporations. Currently available food defense publications can be accessed at the FSIS – [Food Defense and Emergency Response](#) webpage. Some examples are:

- *Developing a Food Defense Plan for Meat and Poultry Slaughter and Processing Plants*: created to assist Federal and State inspected establishments that produce meat and poultry in developing preventive food defense measures. While many establishments may utilize guidelines from other government and private sector organizations and agencies, businesses and establishments that do not have access to this specialized security-planning advice should find these guidelines helpful in improving and preparing food defense plans. These guidelines are currently voluntary, but establishment officials will be well served by adopting and implementing them because they are developed to meet the particular needs of meat, poultry, and egg producing establishments. FSIS has provided these guidelines to its field employees who will assist in directing establishments that seek further clarification or advice.
- *Food Defense Plan – Security Measures for Food Defense*: FSIS has urged establishments to develop functional food defense plans with

control measures to help prevent intentional adulteration of products. A functional food defense plan has the following characteristics:

- it is written
- the measures described in the plan are implemented
- the measures are periodically tested
- the plan is reviewed at least annually and revised if needed

If the establishment is not implementing elements of its plan, IPP cannot take action on that fact because there is no regulatory requirement for such plans.

- *Guidelines for Transportation and Distribution of Meat, Poultry, and Egg Products:* Similar to the “FSIS Security Guidelines for Food Processors,” these guidelines are voluntary and designed to assist small shippers and distributors by providing a list of safety and security measures that these entities should take to strengthen their food safety and food security plans. Protecting food during transportation and storage is a critical component in our defense against all types of food borne contaminants. These guidelines address points in the transportation and distribution process where potential contaminants could be introduced, including loading and unloading, and in-transit storage. FSIS encourages shippers, transporters, distributors, and receivers to develop and implement controls to prevent contamination of products through all phases of distribution, and to have plans in place in the event of accidental or deliberate contamination. Both of these guidelines are available on the FSIS website in several languages.

If you have questions or need clarification about the above referenced materials, you can email the Food Defense Assessment Staff at [FoodDefense@fsis.usda.gov](mailto:FoodDefense@fsis.usda.gov).

## ATTACHMENT 4: Bioterrorism Overview

There are multiple components to bioterrorism. Beyond just agroterrorism, bioterrorism is often defined as the use of biological agents that target humans, plants, or animals; and, was exemplified in anthrax letters that were used in 2001 against the American people. There are also other terrorism components such as conventional, radiological, nuclear, chemical, and cyber, that are typically directed at the human population. This appendix discusses various components of bioterrorism. It is important for the FSIS IPP to be aware of these bioterrorism components from a professional perspective, as well as from the standpoint of serving as a first line of monitoring for animal diseases of great economic significance (e.g., foreign animal diseases). The agents described below could be introduced through an act of terrorism and public health threats that could be introduced through the food supply.

### Types of Agents Used by Terrorists

#### ***Weapons of Mass Destruction:***

Terrorists often use Weapons of Mass Destruction. These include chemical, biological, radiological agents, or high yield explosives. Some examples of chemical weapons used by terrorists are arsenic, cyanide, and pesticides. Examples of biological weapons that terrorists use include anthrax, botulinum, and toxin. Radiological weapons examples used by terrorists include Cesium-137, Strontium-90, and Cobalt-60. When Weapons of Mass Destruction (WMDs) are used, there are four possible areas of impact. They include harm to the economy, disruption of society, psychological disturbance, and political disturbance. Following is a brief discussion of WMD often used by terrorists.

#### **Chemical agents**

Compounds that disrupt body functions used as chemical agents – You should be aware of some of the typical ways in which the chemical agents used by terrorists affect the human body. Here are some examples:

*Vesicants:* Terrorists may use a chemical agent that acts as a vesicant such as a powder. These agents burn and blister the skin or any other part of the body they contact. They act on the eyes, mucous membranes, lungs, skin, and blood-forming organs. They damage the respiratory tract when inhaled and cause vomiting and diarrhea when ingested. Examples of chemical agents that have this effect are *Sulfur mustard* in its pure state is colorless and odorless. It is extremely toxic to the unprotected eyes, skin, and respiratory system. If a victim survives the initial encounter, the mustard continues to destroy the body's immune defenses and can complicate treatment of acquired infection. *Nitrogen mustards* are more

toxic than sulfur mustards and are easily manufactured. Lewisite placed on the skin causes immediate burning sensation, and its odor is readily apparent. Severe damage to the eyes occurs almost immediately after exposure. Lewisite vapors irritate the mucosa of the nasal and upper respiratory system. Lewisite is absorbed into the body, and distributed as a systemic poison to various organs.

*Blood:* Chemical agents also affect the blood. A typical effect of a chemical agent is that they prevent blood from carrying O<sub>2</sub> effectively. For example, *arsenic* can be reacted with zinc and sulfuric acid to form arsine, which is a colorless gas with an unpleasant odor similar to garlic. Arsine is a blood agent but it is referred to as a nerve poisoning due to its secondary effects. Arsine causes the destruction of red blood cells and subsequently the tissues of the kidney, liver, and spleen. Arsine is used today for industrial processing of gallium arsenide chips in the semiconductor industry.

*Choking/Pulmonary:* These chemical agents cause choking and affect the pulmonary system in humans, but they are not food related.

*Incapacitating:* Some chemical agents that can be introduced in food can incapacitate the individuals affected. For example, *BZ*, 3-quinuclidinyl benzylate, is a member of the belladonna group of compound (glycolates) that includes atropine, scopolamine, and many others.

*Emetics:* In many cases, chemical agents, when ingested or inhaled, induce vomiting. Among the vomiting agents that have the most significant effects are diphenylchlorarsine (DA), diphenylcyanoarsine (DC), and adamsite (DM). These agents can be dispersed as aerosols and produce their effects by inhalation. Some minor eye irritation also might occur. Emetics produce a feeling of pain and sense of fullness in the nose and sinuses. This is accompanied by a severe headache, intense burning in the throat, tightness and pain in the chest, irritation of the eyes and lacrimation. Coughing is uncontrollable, and sneezing is violent and persistent. Nausea and vomiting are prominent. Mild symptoms, caused by exposure to very low concentrations, resemble those of a severe cold. The onset of symptoms may be delayed for several minutes after initial exposure, especially with DM. Therefore, effective exposure may occur before the presence of the smoke is suspected. If a protective mask is available and put on by an individual after these symptoms are noticed, the symptoms will increase for several minutes, despite adequate protection. Consequently, the victim may believe the mask to be ineffective, and by removing it, cause further exposure. On leaving the scene of the attack, the victim's symptoms subside rather rapidly, and the severe discomfort vanishes after about one-half hour. At high concentrations, effects may last for several hours. Because of their

arsenical properties, when these chemical agents are introduced, the affected foods become poisonous.

*Tearing:* The chemical agents used for terrorism that cause tearing are not typically introduced through food.

Nerve agents – Some of the nerve agents that can be used by terrorists to affect food products include the following:

- Tabun (GA) - volatile, liquid/vapor
- Sarin (GB) - volatile, liquid/vapor
- Soman (GD) - volatile, liquid/vapor
- VX - low volatility, liquid
- Pesticides - methyl parathion, malathion, diazinon

All of these agents are cholinesterase inhibitors when they are ingested or inhaled. Cholinesterase is an enzyme needed for the proper functioning of the nervous systems of humans, other vertebrates, and insects. They are all pesticides, which act like organophosphates and carbamates to inhibit cholinesterase. Nerve agents are the most toxic and rapidly acting of the known chemical warfare agents. They are similar to pesticides called organophosphates in terms on how they work, and the kinds of harmful effects they cause. However, nerve agents are much more potent than organophosphate pesticides.

Heavy metals – Heavy metals can also be used by terrorists to affect food products. The most dangerous ones include the following:

- Arsenicals
- Mercury
- Cyanide
- Thallium

*Arsenic:* The primary symptoms of acute inorganic arsenic poisoning in humans are painful dysesthesias, decreased deep tendon reflexes, decreased pain, touch, and temperature sensation. Individuals who have arsenic poisoning may also experience nausea, anorexia, vomiting, epigastric and abdominal pain, and diarrhea. These symptoms are so severe that they often end in death. Chronic exposure to low levels of arsenic has led to nasal septum perforation, dermatological symptoms (lesions, necrosis, etc.), and an increase in the incidence of lung and lymphatic cancers.

*Mercury:* The heavy metal mercury is not well absorbed by the human gastro intestinal tract, but there is good pulmonary absorption of mercury vapors, especially methyl mercury.

*Cyanide:* Cyanide is rapidly absorbed from the stomach, lungs, mucosal surfaces, and unbroken skin. It is also a rapidly acting poison that can exist in various chemical forms. Examples of simple cyanide compounds include hydrogen cyanide, sodium cyanide, and potassium cyanide. Hydrogen cyanide is a colorless gas with a faint, bitter, almond-like odor. Sodium cyanide and potassium cyanide are both white solids with a bitter, almond-like odor in damp air. Cyanide and hydrogen cyanide are used in electroplating, metallurgy, production of chemicals, photographic development, making plastics, fumigating ships, and some mining processes. Effects begin within seconds of inhalation and within 30 min of ingestion. A bitter almond odor may be detected on the breath. Later effects include coma, convulsions, paralysis, respiratory depression, pulmonary edema, arrhythmias, bradycardia, and hypotension. Antidotal therapy: Amyl nitrite, sodium nitrite, and sodium thiosulfate with high-dose oxygen should be given as soon as possible.

*Thallium:* Thallium is a toxic heavy metal. Most cases of thallium toxicity occur after oral ingestion. Gastro intestinal decontamination, activated charcoal, and Prussian blue (potassium ferric hexacyanoferrate) are recommended in thallium ingestion.

## **Biological Agents and Toxins**

Before discussing the diseases, it is important to understand the weaponization of an agent. If an agent has been “weaponized”, characteristics of the pathogen may have been altered to make it a more effective weapon. For example:

- the transmission of a pathogen may be enhanced or the virulence increased;
- the organism may have been altered to make it resistant to antibiotics it would otherwise be susceptible to;
- may allow an organism to evade the normal protective immunity induced by vaccine, or it may even alter the clinical signs

However, reviewing the agents and what we currently know about them is still important for our enhanced awareness of these agents.

The CDC divides biological agents and toxins into three categories:

- Category A - High priority
- Category B - Second highest priority
- Category C - Third highest priority

Be aware that the CDC changes the agents listed in these categories as additional information becomes available. Let us discuss each of these in more detail.

## **Category A**

The biological agents and toxins that fall into Category A can be easily disseminated, or transmitted person-to-person. They cause high mortality, with potential for major public health impact. Their introduction might result in public panic, and social disruption. They require special action for public health preparedness. Following are the agents and toxins that are currently listed in Category A:

- Anthrax (*Bacillus anthracis*)
- Botulism (*Clostridium botulinum* toxin)
- Plague (*Yersinia pestis*)
- Smallpox (*Variola major*)
- Tularemia (*Francisella tularensis*)
- Viral hemorrhagic fevers (e.g., Ebola)

### Anthrax

Anthrax results from infection by *Bacillus anthracis*, a spore forming gram-positive aerobic rod. Anthrax can be found as a spore in the soil worldwide; it is particularly common in parts of Africa, Asia, and the Middle East. In the United States, foci of infection occur in South Dakota, Nebraska, Mississippi, Arkansas, Texas, Louisiana, and California, with smaller areas in other states.

Spores can remain viable for decades in the soil or animal products, such as dried or processed hides, and wool. Spores can also survive for 2 years in water, 10 years in milk, and up to 71 years on silk threads. However, the vegetative organisms are thought to be destroyed within a few days during the decomposition of unopened carcasses (exposure to oxygen induces spore formation).

There are three forms of the disease in humans:

1. Cutaneous anthrax that develops after skin infections. This form is characterized by a papular skin lesion, which becomes surrounded by a ring of fluid-filled vesicles. Most lesions (malignant carbuncle) are non-painful and resolve spontaneously; but disseminated, fatal infections occur in approximately 20% of cases.
2. Intestinal anthrax develops after eating contaminated meat. The initial symptoms may be mild malaise and gastrointestinal symptoms. Severe symptoms can develop and rapidly progress to shock, coma, and death.
3. Pulmonary anthrax occurs after inhaling spores in contaminated dust. Natural infections are mainly seen among workers who handle infected hides, wool, and furs (Wool Sorter's Disease). Symptoms may include

fever, tiredness, and malaise; a nonproductive cough and mild chest pain may be present. Thereafter follows an acute onset of severe respiratory distress, with fatal septicemia and shock within one to two days. Fatalities may be prevented if treated early; however when symptoms are flu-like and non-specific, early treatment is not sought.

In animals, sheep, cattle, and horses are very susceptible, while dogs, rats, and chickens are resistant to disease. In ruminants, sudden death may be the only sign. However, the disease may manifest as flu-like symptoms; chronic infections often have edema.

In the 1950's and 1960's, *B. anthracis* was part of the U.S. bioweapons research program. In 1979, there was an accidental release of aerosol anthrax from a military compound in the Soviet Union. The neighboring residents experienced high fevers, difficulty breathing, and a large number died. Fatality estimates ranged from 200-1,000. In 1992, Russian President Boris Yeltsin finally acknowledged that the release occurred from a large-scale military research facility. In 1991, Iraq admitted it had done research on *B. anthracis* as a bioweapon.

There are several characteristics of *B. anthracis* make it attractive as a bioweapon. It is widely available and relatively easy to produce. The spores are infective, resistant, and remain infective when aerosolized. A lethal dose for inhalation of spores is low and mortality is high; the case-fatality rate for inhalational anthrax could approach 100%. Untreated pulmonary and intestinal infections are usually fatal, especially, if recognized too late for effective treatment. Person-to-person transmission of anthrax is very rare and has been reported only in cases of cutaneous anthrax.

Vaccines are available for humans who have a high risk of infection. The efficacy of the vaccine against inhalation of *B. anthracis* is unknown, and reactogenicity of the vaccine is mild to moderate. Vaccines are available for livestock. Natural strains of *B. anthracis* are usually susceptible to a variety of antibiotics, but effective treatment depends on early recognition of the symptoms. Treatment for cutaneous anthrax is usually effective, but pulmonary and intestinal forms are difficult to recognize and mortality rates are much higher. Prophylactic antibiotics are appropriate for all exposed humans. Anthrax spores are resistant to heat, sunlight, drying, and many disinfectants, but are susceptible to sporicidal agents or sterilization.

### Botulism

Toxins produced by *Clostridium botulinum* cause botulism, or "limber neck" in waterfowl. It is a gram positive, spore-forming, toxin-producing obligate anaerobic bacillus. The spores are ubiquitous in soil.

A German physician, Justinus Kerner in 1793, first discovered botulism. He called the substance “wurstgift”, and found it in spoiled sausages. During this period, sausage was made by:

1. filling a pig’s stomach with meat and blood,
2. boiling it in water; then
3. storing it at room temperature, which were ideal conditions for clostridial spores to survive

Botulism gets its name from “botulus”, which is Latin for sausage.

United States federal regulations for food preservation resulted following several outbreaks of botulism. In the U.S., botulism spores germinate and release seven different antigenic types of neurotoxins; classified as A through G. Different neurotoxin types affect different species.

Only a few nanograms of the toxin can cause severe illness; and, all cause flaccid paralysis. Neurologic clinical signs, including generalized weakness, dizziness, dysphagia, and flaccid paralysis are similar in all species affected. In humans, gastrointestinal symptoms may precede the neurologic symptoms because the preformed toxin is ingested. In animals, many species of mammals and birds can be affected. Clinical disease is most often in wildfowl, poultry, mink, cattle, sheep, and horses. Ruminants and horses will often drool, while humans experience dry mouth. Paralysis of the respiratory muscles leading to death may occur in 24 hours in severe cases. Waterfowl are especially sensitive; and pigs, dogs, and cats are fairly resistant.

Botulinum toxins are known to have been weaponized by several countries and terrorist groups in the past. It was part of the U.S. bioweapons program. Iraq has produced large volumes of this toxin, and the Aum Shinrikyo cult in Japan tried to use it unsuccessfully in 1990. The botulinum toxins are relatively easy to produce and transport. Botulinum toxin is extremely potent and lethal; and, is the single most poisonous substance known. Signs of a deliberate release of the toxin; either via aerosol, food, or water, is expected to cause clinical illness similar to food borne illness. Additionally, uncommon toxin types, such as C, D, F, or G, may be the culprits; and thus, raise suspicion of an intentional release.

In endemic areas, toxoids are typically used in horses, cattle, sheep, and goats; and investigational toxoids for high-risk laboratory workers are available. However, these toxoids are not effective for post-exposure prophylaxis. Botulinum antitoxin (trivalent) is sometimes used in animals, but response depends on the type of toxin causing the disease and the species of animal. In humans, if given early, the antitoxin may decrease the severity of disease and shorten the duration of symptoms. It has severe side effects, and is only used on a case-by-case basis. The U.S. Army has an investigational heptavalent antitoxin. Antibiotics may be warranted if a wound is involved, but immediate

intensive care may be the only treatment. Botulinum toxins can be inactivated by sunlight in 1 to 3 hours; as well as bleach, sodium hydroxide, or chlorinated water. The spores are very resistant in the environment but moist heat (120°C for at least 15 min) will destroy them.

### Tularemia

Tularemia, or “rabbit fever”, is caused by *Francisella tularensis*, a gram negative bacteria. The disease can be transmitted by:

- ingestion of infected, undercooked meat (rabbit);
- bites from infected ticks, and less commonly deerflies;
- through direct contact with blood or tissues of infected animals (especially rabbits); and
- inhalation of contaminated dust

Initial symptoms are flu-like; and they include fever, chills, headache, and myalgia. In humans, there are six clinical forms of tularemia – glandular and ulceroglandular are the most common presentation of this disease. An ulcer may or may not be present at site of infection, and local lymph nodes are enlarged.

Oculoglandular occurs when conjunctiva become infected by rubbing eyes with contaminated fingers, or by splashing contaminated materials in the eyes. The oropharyngeal presentation is caused by ingestion of organism in contaminated food (undercooked meat), or water.

Typhoidal and pneumonic forms usually occur following inhalation, or hematogenous spread of the organism. Both of these forms tend to present as atypical pneumonia; and most fatalities occur with these forms, and can be as high as 30-60% if untreated.

In animals, the full spectrum of clinical signs is not known. Sheep, young pigs, horses, dogs, and cats are susceptible to tularemia. Signs of septicemia such as fever, lethargy, anorexia, and coughing are most commonly seen. In wildlife, clinical disease is not often seen and animals are found dead or moribund. However, when infected hares and cottontails are observed, they behave strangely in that they are easily captured because they run slowly, rub their noses and feet on the ground, experience muscle twitch, are anorectic, have diarrhea, and are dyspneic. These lagomorphs are an important reservoir for human infection. Older swine and bovine seem to be resistant to disease and are asymptomatic.

In the 1950-60's, the United States military developed weapons that aerosolized *F. tularensis*, and it is suspected that other countries may have included this organism in their bioweapons research program as well. There are many characteristics that make *F. tularensis* a good agent for bioterrorism. It is stable,

survives in mud, water, and dead animals for long periods of time; and, has previously been stabilized as a bioweapon. Only a low dose is needed to cause inhalational disease. Case fatality rates of the typhoidal and pneumonic forms are reported to be 30-60% if untreated. In 1969, the World Health Organization (WHO) estimated that if 50kg of virulent *F. tularensis* particles were aerosolized over a city with 5 million people, the result would be 250,000 illnesses and 19,000 deaths. Recently, the CDC estimated the economic losses associated with an outbreak of tularemia to be \$5.4 billion for every 100,000 people exposed.

Person-to-person transmission has not been documented with a tularemia infection; so, secondary spread is of little concern. However, infectious organisms can be found in blood and other tissues; care must be taken when handling infected material. Antibiotics are generally effective if given early in the infectious process, and as a prophylaxis. There is a live attenuated vaccine (given intradermally or by scarification) that is available to individuals at high risk for exposure to the bacteria. The vaccine's efficacy against high dose respiratory challenge is unknown. Disinfection of the bacteria is easily accomplished with many common disinfectants. However, the bacteria are stable at freezing temperatures for months to years.

### **Category B**

The biological agents and toxins that fall into Category B are moderately easy to disseminate. They cause moderate morbidity, and low mortality. They require specific enhancements of the CDC's diagnostic capacity, and enhanced disease surveillance. The following agents and toxins are in Category B:

- Brucellosis (*Brucella* spp)
- Epsilon toxin (*Clostridium perfringens*)
- Food threats (*Salmonella*, *E. coli* O157:H7, *Shigella*)
- Glanders (*Burkholderia mallei*)
- Melioidosis (*Burkholderia pseudomallei*)
- Psittacosis (*Chlamydia psittaci*)
- Q Fever (*Coxiella burnetii*)
- Ricin toxin (castor beans)
- Staphylococcal enterotoxin
- Typhus (*Rickettsia prowazekii*)
- Viral encephalitis (VEE, WEE, EEE)
- Water safety threats (*Vibrio cholera*, *Cryptosporidium parvum*)

### Brucellosis

Brucellosis, or undulant fever, is caused by various species of *Brucella*, a gram negative, facultative intracellular rod. The organism can persist in the

environment and indefinitely if frozen in aborted fetuses or placentas.  
Transmission occurs via

- Ingestion-of infected food, or consuming infected unpasteurized milk or dairy products,
- Inhalation-of infectious aerosols (a means of infection in abattoirs); or
- Contact with infected tissues through a break in the skin or mucous membranes.

Brucellosis can involve any organ or organ system, and have a very insidious onset with varying clinical signs. The one common sign in all patients is an intermittent/irregular fever with variable duration; thus, the term undulant fever.

There are three forms of the disease in humans. In the acute form (<8 weeks from illness onset), symptomatic, nonspecific, and flu-like symptoms occur. The undulant form (< 1 yr. from illness onset and symptoms) include undulant fevers, and arthritis. In the chronic form (>1 yr. from onset), symptoms may include chronic fatigue-like syndrome and depressive episodes. Illness in people can be very protracted and painful; and can result in an inability to work, and loss of income. In animals, the clinical signs are mainly reproductive in nature, such as abortions, epididymitis, orchitis, and fistulous withers in horses.

The following indicates the specific brucellosis species, host, and human pathogenicity:

- *B. abortus* > cattle, bison, elk or horses > yes
- *B. melitensis* > goats, sheep or cattle > yes
- *B. suis* > swine, hares, reindeer, caribou, or rodents > yes
- *B. canis* > dogs, or other canids > yes
- *B. ovis* > sheep > no

In the 1950's when the U.S. bioweapons research program was active, *Brucella suis* was the first agent weaponized. The World Health Organization prepared a bioterrorism scenario looking at aerosolized *B. melitensis* (which has more serious consequences for humans than *B. suis*) spread along a line with the prevailing winds with optimal meteorological conditions. It was assumed that the infectious dose to infect 50 (ID50) percent of the population would require inhalation of 1,000 vegetative cells. The case fatality rate was estimated to be 0.5% with 50% of the people being hospitalized and staying an average of seven days. It is highly infective, and fairly stable in this form. Incubation period in humans is one week up to several months, which often complicates the diagnosis due to the latency of clinical signs. Person-to-person transmission is very rare.

Prolonged antibiotics are necessary to penetrate these facultative intracellular pathogens. Combination therapy has shown the best efficacy for treatment in

humans. Vaccinating calves has helped eliminate infection in these animals, thus decreasing possible exposure to humans. Strict adherence to federal laws of identifying, segregating and/or culling infected animals is essential to success. Properly protect yourself to prevent exposure to tissues and body secretions of infected animals by wearing gloves, masks, goggles, and coveralls. Pasteurization or boiling milk and avoidance of unpasteurized dairy products will help decrease human exposure to brucellosis. The organism is susceptible to many disinfectants.

### Equine Encephalitis

Encephalitis is the only viral group in the list of Category B agents. This group of equine encephalitis viruses is RNA viruses in the Alphavirus genus. Eastern, Western, and Venezuelan Equine Encephalitis viruses are transmitted by mosquitoes.

The female mosquito takes a blood meal from a viremic host, generally birds for EEE and WEE, and birds and horses for VEE. The virus replicates in the salivary glands of the mosquito and is transmitted back to birds or to dead end hosts, such as humans and horses, where overt disease occurs. In humans, infections can be asymptomatic or cause flu-like illness. In a small proportion of cases viral encephalitis can occur, and lead to permanent neurological damage or death.

Horses, donkeys and mules have similar clinical signs as humans. The disease in these animals often precedes human cases by several weeks. EEE and VEE have mortality rates of 40-90%; WEE has a lower mortality rate, ranging from 20-30%. Birds are asymptomatic carriers. The detection of viremia in sentinel birds is detected via ELISA.

VEE was tested in the U.S. bioweapons program in the 1950s and 1960s. It is thought that other countries have also weaponized VEE. All U.S. stocks of VEE were destroyed, along with the other agents that were part of the program. VEE can be produced in large amounts by unsophisticated and inexpensive systems. The virus can be aerosolized, or spread by releasing infected mosquitoes. Humans are highly susceptible. Approximately 90-100% of exposed individuals could become infected and have clinical signs, although most are mild. Equids would also be susceptible, and disease would occur simultaneously with human disease. There is a low overall human case-fatality rate.

Antibiotics are not effective for treatment, and there are no effective antiviral drugs available. Treatment involves supportive care. There is a trivalent formalin inactivated vaccine available for horses for WEE, EEE, VEE in the United States; but the human vaccines is limited to those who are researchers, and at a high risk of exposure. All of the virus types are unstable in the environment.

## **Category C**

The agents that fall into Category C include emerging pathogens that could be engineered for mass dissemination in the future because of availability, ease of production and dissemination, the potential for high morbidity and mortality rates, and major health impact. Following are the agents that fall into Category C:

- Nipah virus
- Hanta virus

### Nipah

Nipah virus (a Paramyxovirus) was discovered in Malaysia in 1999, and causes a severe respiratory disease in pigs and severe encephalitis in humans. The reservoir for the virus is thought to be fruit bats, which are called flying foxes. Suspected transmission of the virus occurs from bats roosting in fruit trees close to pig confinements. The virus then spreads rapidly through the swineherd by direct contact, or aerosolization (usually coughing). It can then be passed to humans, dogs, cats and other species.

Transmission can also occur from direct contact with infected body fluids. To date, no person-to-person, or bat-to-person transmission, has been reported. In humans, the incubation period is 3-14 days. Initial symptoms include fever, headache, dizziness, drowsiness, disorientation and vomiting. Some cases show signs of respiratory illness. In severe cases, rapidly progressive encephalitis can occur, with a mortality rate of 40%.

In swine, Nipah virus is highly contagious and easily spread. Many pigs are asymptomatic. Clinical signs include acute fever (>104° F), tachypnea and dyspnea with open mouth breathing, and a loud, explosive barking cough may also be noted. Occasionally, neurological signs can occur. Clinical signs in pigs were noted 1-2 weeks before illness in humans making swine a sentinel for human disease. Disease in other animal species is poorly documented. Other species demonstrate respiratory and neurological signs.

Nipah virus is described as an emerging pathogen with potentially high morbidity and mortality, as well as a major health impact. Currently transmission of the disease involves close contact with pigs, but aerosolization may be a possible bioterrorism method of dispersal. The potential for this virus to infect a wide range of hosts and produce significant mortality in humans makes this virus a public health concern.

Nipah virus is a very dangerous pathogen and is classified as a Biolevel 4 agent. If you suspect an outbreak, contact your state veterinarian and state public health veterinarian IMMEDIATELY! Avoid all contact with potentially infected species

(pigs, dogs, cats) until the proper authorities are consulted. Detergents can readily inactivate Nipah virus. Routine cleaning and disinfection with sodium hypochlorite, or several commercially available detergents, is expected to be effective.

### **Radiological/Nuclear Agents**

“Nuclear” involves a fission reaction (nuclear weapon, nuclear power plant, satellites, and waste processing facility). It requires special nuclear material, such as plutonium and/or uranium. “Radiological” involves radionuclides, which can be dispersed or deposited. Accidents such as the reactors at Three Mile Island in Pennsylvania (small release) and Chernobyl in Russia (large catastrophic release), have taught us about the effects on the agriculture and the food supply. Those lessons focus on making decisions to evacuate if establishment conditions worsen or remain unstable. Additionally, the federal government has extensive plans, and practices emergency response around nuclear facilities in the U.S.

### **Targets and Pathways**

There are many methods of delivery and points in the agriculture process that an agent could be introduced. Covert, or stealth, introductions will go unnoticed for a longer period than overt introduction because we will be treating it as if it occurred under natural conditions. The simultaneous release of three to four highly contagious, foreign animal pathogens in several locations around the country at key points would be overwhelming.

High-density population areas represent tempting terrorist targets. Most lack even rudimentary monitoring capabilities. Some examples include:

- Urban population centers,
- Business centers,
- Transportation nodes,
- Special events (e.g., political conventions, Super Bowl, Olympics, etc.), or
- Agribusiness and national food supply infrastructure.

Terrorists can exploit multiple pathways. They can introduce biological, radiological, chemical, or other types of harmful agents into the population in a variety of ways, including:

- Air dispersion (line and point source),
- Public transportation,
- Water supplies,
- Food distribution systems, and
- Mail distribution systems

## **Consequences**

While the topic of food defense is highly concerned with the intentional introduction of foreign agents, there is the possibility that international travelers might bring one or more microbial agents into the U.S. accidentally. At first onset, an intentional outbreak of a disease in animals or crops is hard to differentiate from a natural outbreak, which delays finding the true source. False claims and hoaxes can be introduced to diminish public confidence in food safety for particular commodities or products. A false report of one case of BSE occurring in the U.S. would send the beef industry into a tailspin for a brief time, losing perhaps tens of millions of dollars or more in overall costs. Foreign trading partners might hear of the rumor and implement a trade ban. The perpetrator relies upon the media to do the damage for him/her by spreading the rumors and presenting fiction as fact. Clues generated by an outbreak might point toward an intentional introduction.

The impact and consequences from a foreign animal disease such as Foot and Mouth Disease (FMD) in the U.S. could be severe. Harsh restrictions on movement would be enacted. We would see road closures, quarantined farms, and animal movement ceased. Access to campsites, state parks, wilderness areas, lakes, city parks, and zoos may be denied.

The psychological impact and mental health of livestock producers, veterinarians and the local community could be negatively affected if entire herds are quarantined and destroyed. The public could be shocked by some of the images the outbreak produces, and alter their buying habits as consumers. It is unlikely that a terrorist attack would create mass food shortages, but movement restrictions could complicate availability temporarily.