



United States
Department of
Agriculture

Food Safety and Inspection Service

Food Defense Guidelines for the Transportation and Distribution of Meat, Poultry, and Processed Egg Products



Revised September 2013

This Publication supersedes *FSIS Food Safety and Security Guidelines for the Transportation and Distribution of Meat, Poultry, and Egg Products*.

Table of Contents

Food Defense During Transportation and Distribution of Meat, Poultry, and Processed Egg Products	5
What is Food Defense?	5
Who Might Intentionally Contaminate a Food Product?	6
Why is the Transportation of Food a Concern?	6
General Guidelines for Transportation and Distribution	7
Personnel Security and Training	8
Secure Facility and Monitor Operations	9
Access	9
Shipping/Receiving	10
Off-Hour Deliveries	11

Table of Contents

Inspection	11
Transport Vehicle and Container Security	13
Shipping	13
Receiving	13
Multiple Stop Shipments	14
Inspecting/Securing/Locking	14
Contingency Issues	14
Tamper-Evident/Resistant Packaging and Coded Labels	16
Emergency Response Procedures	17
Additional Guidance for Highway, Aviation, Maritime, and Rail	18
Imports: Customs Trade Partnership Against Terrorism (C-TPAT)	20
Food Defense Plan	21
Food Defense Plan Elements	22
Resources & More Information	25

The FSIS *Food Defense Guidelines for the Transportation and Distribution of Meat, Poultry, and Processed Egg Products* is designed to assist those handling food products during transportation and storage. These guidelines provide a list of defense measures that can be taken to prevent intentional contamination of meat, poultry, and processed egg products during loading, unloading, transportation, and in-transit storage.

FSIS strongly encourages shippers, receivers, transporters, and importers of these products to develop controls for ensuring the condition and integrity of the products through all phases of distribution. Such controls are necessary to protect the products from intentional contamination. Note that many measures to prevent intentional contamination also help prevent unintentional contamination.

These guidelines address security measures specifically intended to prevent intentional contamination due to criminal or terrorist acts. They apply to all points of shipment of the products—from the processor to delivery at the retail store, restaurant, or other facility serving consumers.

FSIS recognizes that not all of the guidelines contained in this document will be appropriate or practical for every transporter or distributor. Operators should review the guidelines in each section that relate to a component of their operation and assess which preventive measures are suitable. It is recommended that operators consider the goal of the preventive measure, assess whether the goal applies to their operation, and, if so, determine the most efficient and effective way to accomplish the goal for their operation.

FSIS encourages industry to also use additional FSIS food defense guidance and tools that address other operations at slaughterhouses, processing plants, shipping companies, distribution centers, warehouse facilities, and import establishments. These guidance materials can be accessed at www.fsis.usda.gov.

Links to additional guidance, developed by USDA and others, are listed at the end of this booklet.

If you have questions or need clarification about these guidelines, please contact the FSIS Policy Development Division at 1-800-233-3935 or the Small Plant Help Desk at 1-877-FSIS-HELP (877-374-7435).

Food Defense During Transportation and Distribution of Meat, Poultry, and Processed Egg Products

The tragic events of September 11, 2001, forever changed our world. They proved to us that the unthinkable could become reality, and that threats to our Nation's food supply are very plausible from those who want to harm us. Since the terrorist attacks on America, security—including food defense—has been the highest priority at both the Federal and State levels.

Ensuring safe food, along all points in the food supply chain, is a vital function in protecting public health. We must now look at all possible threats, examine the risks, and take action to prevent any intentional attacks using the food supply to cause harm.

What is Food Defense?

Food defense is putting measures in places that reduce the chances of criminals or terrorist groups intentionally contaminating the food supply with a variety of harmful substances. These substances could include materials that are not naturally occurring or not routinely tested for in food products. The goals of those who contaminate food might be to kill people, disrupt our economy, or ruin your business. Intentional acts generally occur infrequently, can be difficult to detect, and are hard to predict. As such, food defense addresses additional factors to include physical security, inside security, and personnel security.

Food defense is **not** the same as food safety. Food safety addresses the unintentional adulteration of food products. Food defense is the protection of food products from intentional contamination.

To help owners and operators of **processing establishments, warehouse and distribution centers, importers, and food transportation companies**, the United States Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) has created this guide to assist you in further protecting the U.S. food supply. It was developed in consultation with industry representatives to ensure that the information presented is beneficial, practical, and achievable.

FSIS recommends you review the guide and assess which preventive measures are suitable for your operation. You should determine the most cost-effective way to achieve food defense goals based on your situation. **It is important to remember that not all measures will be appropriate for every establishment or operation.**

Who Might Intentionally Contaminate a Food Product?

The following are some examples of the types of individuals who might be motivated to intentionally contaminate food products:

- ❖ Members of extremist or activist groups posing as:
 - ◆ Truck drivers (shipping and receiving)
 - ◆ Contractors
 - ◆ Temporary employees
 - ◆ Cleaning crew employees
 - ◆ Visitors
 - ◆ Utility representatives

Another threat may come from an internal source, such as disgruntled current or former employees and other insiders, who typically know what procedures are followed in your operations and often know how to bypass many security controls that would detect or delay an outside intruder.

You should contact your local law enforcement officials to discuss potential local threats to your facility.

Access additional information on the insider threat at http://www.tsa.gov/what_we_do/tsnm/highway/documents_reports.shtm#brochures.

Why is the Transportation of Food a Concern?

FSIS has conducted numerous vulnerability assessments on various commodity systems. In all of these assessments, the transportation phase was identified as a critical vulnerable point of the food supply chain.

Reasons:

- ❖ Food products are more accessible during transportation.
- ❖ Potential for unobserved access to food products is greater.
- ❖ Safeguards are more difficult to implement as the environment is less controlled.

General Guidelines for Transportation and Distribution

Meat, poultry, processed egg products, and ingredients that go into these products are susceptible to intentional contamination from a wide variety of physical, chemical, biological, and radiological agents. Everyone in the food distribution system is responsible for ensuring that these products are safe, wholesome, and unadulterated. Therefore, as part of this system, those responsible for transportation and delivery should implement food defense measures to ensure the safety and security of the products throughout the supply chain.

The following are recommended security measures that processing plants, shipping companies, and warehouses can implement to minimize the risk of tampering or other criminal actions during transportation.



Personnel Security and Training

- ❖ Conduct background and criminal checks:
 - ◆ Make appropriate to staff positions; verify references (including contract, temporary, custodial, seasonal, and security personnel).
 - ◆ Consider using a nationwide database system for facility staff and drivers.

When this is not practical, such personnel (e.g., day laborers) should be under constant supervision and their access to sensitive areas of the facility restricted.

- ❖ Maintain the highest standards for employees working in sensitive areas and who may be alone with product.
- ❖ Require, by contract, that domestic and foreign suppliers (processors and transporters) conduct background checks on staff/drivers and closely monitor transportation operations.
- ❖ Determine employment eligibility; consider using the free U.S. Citizenship and Immigration Services (USCIS) programs (1-888-464-4218) or E-Verify (http://www.dhs.gov/files/programs/gc_1185221678150.shtm).
- ❖ Train all employees on how to detect and report suspicious activities, such as product tampering, so they can recognize threats to security and respond appropriately.
 - ◆ Have a tracking system in place for these reports and follow-up activities.
 - ◆ Ensure employees know emergency procedures and contact information.
- ❖ Take measures to ensure imported meat, poultry and egg products are presented to FSIS for reinspection prior to entering U.S. commerce as required.
- ❖ Ensure that “U.S. Returned” exported products are approved by FSIS for return to the United States.
- ❖ Train personnel involved in the transportation, handling, and storage of meat, poultry, and processed egg products in procedures that will ensure the protection of these products. (For example, train dock and security personnel on documentation requirements for incoming and outgoing shipments.)
- ❖ Promote ongoing security consciousness, the importance of security procedures, and a workplace-watch approach with personnel.

Secure Facility and Monitor Operations

- ❖ Implement a “workplace-watch” approach.
 - ◆ Encourage employees to report any suspicious activities, such as signs of possible product tampering.
 - ◆ Have a tracking system in place for these reports and a procedure for follow-up actions.
 - ◆ Be aware of and report any suspicious activity to appropriate authorities. (Unscheduled maintenance, deliveries, or visitors should be considered suspicious.)
- ❖ Watch sensitive areas closely, ideally utilizing closed-circuit televisions and video cameras.
- ❖ Ensure adequate interior and exterior lighting at the facility.

Access

- ❖ Maintain a positive identification (ID) system for employees. Require identification for and escort temporary visitors at all times while on the premises.
- ❖ Ensure clear identification of personnel and their specific functions (e.g., colored hats or aprons, ID cards).
- ❖ Restrict types of personal items allowed in the establishment, especially firearms or other weapons.
- ❖ Secure and restrict access to facilities, transportation trucks, trailers, containers, locker rooms, and all storage areas with alarms, cameras, locks, fences, or other appropriate measures to prevent access by unauthorized persons.
- ❖ Establish procedures for handling unauthorized persons in a restricted-access area.
- ❖ Establish policy and procedures for allowing rail crew, truckers, etc., to enter the facility. Monitor their activities while they are on the property. Restrict them to non-product areas unless they are an employee.

- ❖ Limit access to:
 - ◆ food delivery, storage, food ingredient, and chemical storage areas;
 - ◆ outside water tanks, water supplies, ice machines, and water pipes;
 - ◆ central controls for heating, ventilation, and air conditioning (HVAC); electricity; gas; and steam systems to prevent contamination from entering the air-distribution systems.
- ❖ Enhance software and control systems:
 - ◆ ensure that you have anti-virus software and firewalls installed, properly configured, and up to date;
 - ◆ update operating systems and critical program software, as well as backing up key files;
 - ◆ do not allow unauthorized external storage devices access to your network and systems.
- ❖ Designate limited and specific entry and exit points for people and trucks.
- ❖ Secure all transportation operations—doors, vent openings, windows, outside refrigeration and storage units, trailer bodies, and bulk storage tanks.
- ❖ Designate parking areas for visitors away from the main facility, if practical. Vehicles of employees and visitors should be clearly marked (e.g., placards, decals). This is intended to identify vehicles authorized to be on the premises and deter bombing attempts.

Shipping/Receiving

- ❖ Identify and monitor sensitive transportation operations, such as food loading and unloading areas, especially where temporary employees who have not had background checks are working.
- ❖ Control the storage of food shipping containers and liners. If possible, keep them in an area that can be locked until needed.
- ❖ Develop a checklist for shipping and receiving procedures. Using a checklist can help identify unusual activities.
- ❖ Secure loading docks to prevent unauthorized access or deliveries.
- ❖ Check all deliveries against a roster of scheduled deliveries. Truck drivers should show proper identification upon arrival.
- ❖ Ensure seal program requirements are followed as described in the “Transport Vehicle and Container Security” section.

- ❖ Monitor transport vehicles when picking up a load from a warehouse especially when trailer or container doors are open.
- ❖ Purchase food ingredients, food products, and packaging materials from known, reputable suppliers. Require Letters of Guaranty, if possible.
- ❖ Hold unscheduled deliveries outside the premises pending verification of the shipper and cargo. Do not accept deliveries from, or release product to, unknown shippers that use only cell phone numbers or known shippers with unknown phone/fax numbers or email addresses.

Off-Hour Deliveries

- ❖ Require prior notice from suppliers (by phone, email, or fax) for deliveries outside of normal operating hours.
- ❖ Require the presence of authorized company personnel to verify and receive delivery.
- ❖ Supervise loading and unloading of products, ingredients, packaging, labels, and product returns.

Inspection

- ❖ Examine incoming products and their containers for evidence of tampering or intentional contamination, such as torn boxes/bags and cut tape. Pay special visual attention to less-than-load (LTL) or partial load shipments.
- ❖ Develop and implement methods to check and document the condition of the product and packaging upon receipt at the destination.
- ❖ Establish policy and procedures for the rejection of packages and products that are not acceptable, cannot be verified against the delivery roster, or contain unacceptable changes to shipping documents. Have a monitoring strategy and recordkeeping system in place to document actions taken.
- ❖ Note on the bill of lading any problems with the condition of the product, packaging, labels, and seals.
- ❖ Do not accept products that are known or suspected of being intentionally contaminated.

- ❖ Check food for unusual odor or appearance.
- ❖ Processors may want to arrange with receivers to sample and conduct microbiological or other tests on products with extended shelf-life potential. The following items should be included in a testing plan:
 - ◆ In-house testing would be required prior to shipment.
 - ◆ Results should be compared with pre-shipment results to determine whether adjustments are needed in transport methods or procedures.
 - ◆ Chain-of-custody procedures providing for the proper handling of samples should be established.
 - ◆ Samples should be clearly marked and kept in a secure area.
 - ◆ All tested products should be held pending results.



Transport Vehicle and Container Security

- ❖ Have a strictly enforced seal program.
 - ◆ Identify and require seal specifications (e.g., tamper-proof, numbered seals, etc.).

Shipping

- ❖ Inspect shipping containers closely for any evidence of tampering.
- ❖ Apply seals to all tankers, trucks, or containers being shipped and maintain a logbook of seal assignments. Record seal number and trailer numbers on the shipping documents (e.g., bill of lading, load manifest, or certificate). Have a system in place to verify seal numbers and the integrity of the seals throughout the distribution process. Maintain a bill of lading for all outbound activity. Keep records of all seal activity.
- ❖ Ensure that shipping documents also contain product information, name of carrier(s), and driver information.

Receiving

- ❖ Require that incoming shipments/deliveries be sealed and ensure that the seal number and trailer numbers are recorded on the shipping documents (e.g., bill of lading, load manifest, or certificate) for verification prior to entry to the facility.
- ❖ Require that only a supervisor or an agent of the owner be allowed to break seals and sign off in the driver's logbook.
- ❖ Maintain an inbound load verification logbook/bill of ladings.
- ❖ Ensure that shipping documents also contain product information, name of carrier(s), driver information.

❖ **Multiple Stop Shipments**

- ❖ Develop procedures for verifying the resealing of shipping conveyances at the time of departure. For example, evaluate the bill of lading for shipper, State and/or Federal seals to ensure the original seal numbers, or new seals applied at a previous stop, match the paperwork.
- ❖ Verification of the last company seal, or government seal for import/export products, put on a shipping conveyance should be available throughout the delivery chain.
- ❖ Multiple stops or less-than-load (LTL) shipments should be kept to a minimum.
- ❖ The shipping conveyance should be kept locked at all times when the operator is not present.

Inspecting/Securing/Locking

- ❖ Inspect transportation trucks, trailers, and containers prior to loading and unloading.
- ❖ Lock or seal transportation trucks, trailers, and containers when not in use, during meal breaks, and at night.
- ❖ Monitor trucks, trailers and containers when doors are open.
- ❖ Secure trucks, trailers, and containers after loading/unloading is complete.

Contingency Issues

- ❖ Have a system in place to ensure the integrity of product when the seal needs to be broken prior to delivery due to multiple deliveries or for inspection by government officials. Document each time the seal is broken.
- ❖ Investigate shipping documents with suspicious alterations immediately. Hold and segregate the product during the investigation.
- ❖ Establish policies and procedures for unacceptable changes to shipping documents. Have a monitoring strategy and recordkeeping system in place to document steps taken.

- ❖ Require that the warehouse supervisor note on the bill of lading any problems with the condition of the product, packaging, labels, and seals.
- ❖ Ensure employees know how to respond to a broken seal and to understand that this is a potentially serious problem.
- ❖ Use truck tracking technology that integrates seal activity to help minimize the opportunity for intentional product contamination.
- ❖ Use Global Positioning Satellite (GPS) technology when possible to track the vehicle's prior destinations before taking delivery.
- ❖ Have response procedures in place when a truck is missing or not in communication for a specified period of time.
- ❖ Ensure that security procedures are also in effect during interim storage at in-transit warehouses.
- ❖ Remove, if possible, transport vehicle (cab and container) labeling that shows it contains food product.



Tamper-Evident/Resistant Packaging and Coded Labels

- ❖ Use tamper-evident/resistant packaging for food bins, boxes, and spouts/fill ports in transit.
- ❖ Use internal and external packaging so customers will be able to determine if the product was tampered with and can immediately notify you. Provide instructions and contact information with shipment.
- ❖ Code product labels so that if an aggressor gains access to the product, he/she will not know what it is or its destination.



Emergency Response Procedures

- ❖ Be aware of and report suspicious activity to appropriate authorities (such as unscheduled maintenance, deliveries, or unknown visitors).
- ❖ Develop procedures for the notification of appropriate authorities if a food-related emergency or suspicious incident occurs. In the event of a food defense emergency, notify local law enforcement first. Then notify the FSIS Office of Program Evaluation, Enforcement and Review regional office. (See contact information at the back of this booklet.)
- ❖ Check your State notification requirements for their recommended notification sequence. Also, keep an up-to-date list of local, State, and Federal emergency contacts; local Homeland Security contacts; and local public health official contacts. You are encouraged to establish these relationships in advance.
- ❖ Investigate threats or reports of suspicious activity swiftly and aggressively.
- ❖ Develop procedures for the safe handling and disposal of contaminated products. Identify where and how to separate suspected products before salvage to allow for investigation and discovery of evidence.
- ❖ Develop procedures for handling threats and actual cases of product tampering.
- ❖ Maintain records for returned goods.
- ❖ Processors, transportation managers, and wholesale and retail distributors should ensure the traceability and recall of products.
- ❖ Keep good records for trace-back and trace-forward as they are essential to contain the impact of an incident.
- ❖ Discuss security and response plans with shipper(s) to ensure they are aligned.
- ❖ Ensure that emergency contact procedures are in place. Include facility personnel, as well as shipper and customer contacts.
- ❖ Have procedures in place for proper evidence control when tampering is suspected.
 - ◆ Discuss the appropriate procedures to be followed to maintain control and chain-of-custody of potential evidence with local law enforcement, the USDA Office of Inspector General, or local Federal Bureau of Investigation (FBI) Weapons of Mass Destruction Coordinator contacts.

Additional Guidance for Highway, Aviation, Maritime, and Rail

Highway

- ❖ Participate in the Department of Homeland Security's (DHS) "First Observer Program" at www.FirstObserver.com. This program's mission is to administer a voluntary anti-terrorism and security awareness program for highway professionals. A key component of the program is to recruit volunteers (e.g., truck and bus drivers) to act as "First Observers" in reporting suspicious criminal or terroristic activities. This program includes an Information Sharing and Analysis Center (ISAC) and coordinates training. You can request to receive security alerts through this program.
- ❖ Ensure that persons handling processed egg products contact the United Egg Association to obtain their 2005 Policy on Tanker Security. (www.unitedegg.org/ContactUEP/default.cfm)

Aviation

An increasing amount of meat, poultry, and processed egg products are being transported by air, so it is critical to ensure the security of these products when this mode of transport is utilized.

- ❖ Check all trucks for signs of tampering before they are admitted to a terminal facility when they are delivering or picking up a shipment.
- ❖ Report suspicious or inconsistent servicing of a container to terminal security.
- ❖ Adhere to Transportation Security Administration (TSA) requirements for screening cargo for aircraft. Information on this program may be found at www.tsa.gov/what_we_do/layers/aircargo/certified_screening.shtm.

Maritime

Ports are vulnerable due to their size, accessibility by water and land, location in metropolitan areas, and the quantity of products moving through them. Approximately 80 percent of U.S. imports arrive via American seaports, yet the U.S. Customs and Border Protection (CBP) physically inspects only a fraction of all containers; the remainder are electronically screened. Therefore, enhanced security measures are necessary for products shipped by sea.

- ❖ Report suspicious or inconsistent servicing of a container to terminal security.
- ❖ Remove seals only in the presence of terminal personnel so the seal number and integrity can be verified.

- ❖ Supervise the opening of ship hatches.
- ❖ Require that shipping line agents provide importers and customs brokers with a record of vessel discharge and checks at discharge and in transit.
- ❖ Establish policies and procedures to download reefer electronic information during inspection. (This will also allow for the identification of unusual activities.)
- ❖ Have a reporting system in place when the discharging of any product looks suspicious or the product shows evidence of tampering.
- ❖ Ensure that the terminal facility is locked during meal breaks and at night.
- ❖ Ensure that facility doors are closed immediately after the truck/trailer has pulled away from the dock.

Rail

Rail transportation is an integral part of the domestic food distribution system; therefore, it is important to recognize that unsecured containers can be easy targets for tampering and to address this vulnerability.

- ❖ Report suspicious or inconsistent servicing of a container to terminal security.
- ❖ Use boxcars dedicated for food products.
- ❖ Employ measures to secure loaded and empty containers from tampering when they are being stored at the train yard.
- ❖ Inspect locks/seals on boxcars for signs of tampering at pull and place.
- ❖ Review shipping documents upon arrival at the train yard and before the train engineer leaves.
- ❖ Inspect the integrity of seals upon arrival and before departure of the load.

Imports: Customs Trade Partnership Against Terrorism (C-TPAT)

If you import food products into the United States, FSIS encourages participation in the C-TPAT program. C-TPAT is a voluntary partnership between the U.S. Government and private sector to strengthen the supply chain security of trade products. C-TPAT is managed by the CBP. Participating companies must:

- ◆ Document their risks throughout their supply chain through a comprehensive security assessment which is verified by C-TPAT, and
- ◆ Implement and maintain security measures.
- ❖ Benefits include expedited customs processing upon entry.
- ❖ More information is available at http://cbp.gov/xp/cgov/trade/cargo_security/ctpat or contact the CBP Industry Partnership Programs at (202) 344-1180, fax: (202) 344-2626, or by email at industry.partnership@dhs.gov.



Food Defense Plan

Previous sections have identified security measures that food processors, importers, transporters, and distributors can take to help prevent the intentional contamination of food products. FSIS recommends that the measures a processor, importer, transporter, or distributor implements be included in a Food Defense Plan.

What is a Food Defense Plan?

A Food Defense Plan is a written document that helps owners and operators of slaughter and processing establishments, warehouse and distribution centers, importers, and food transportation companies identify measures that they have taken to minimize the risk that food products will be intentionally contaminated or tampered with during each phase of the food supply chain – in this case, during transportation and distribution. It sets out the steps that the establishment or facility will take in case there is an intentional contamination incident or emergency.

Why Develop a Food Defense Plan?

There are many potential benefits of having a functional food defense plan in place. A food defense plan:

- ❖ protects public health and business assets;
- ❖ increases confidence among customers, trading partners, and the public;
- ❖ provides a value-added component to your product;
- ❖ deters theft and tampering;
- ❖ creates production and distribution efficiencies;
- ❖ maintains greater control over product throughout the supply chain; and
- ❖ may reduce insurance premiums and freight rates.

Having a food defense plan in place also increases preparedness and may be particularly helpful during emergencies. During a crisis, when stress is high and response time is at a premium, a documented set of procedures improves your ability to respond quickly. **The bottom line is that a food defense plan will help maintain a safe working environment for employees, provide a safe product to customers, and protect your business. It is essential that food transportation and distribution be included in your food defense plan.**

Food Defense Plan Elements

There are four key elements that make up a functional food defense plan:

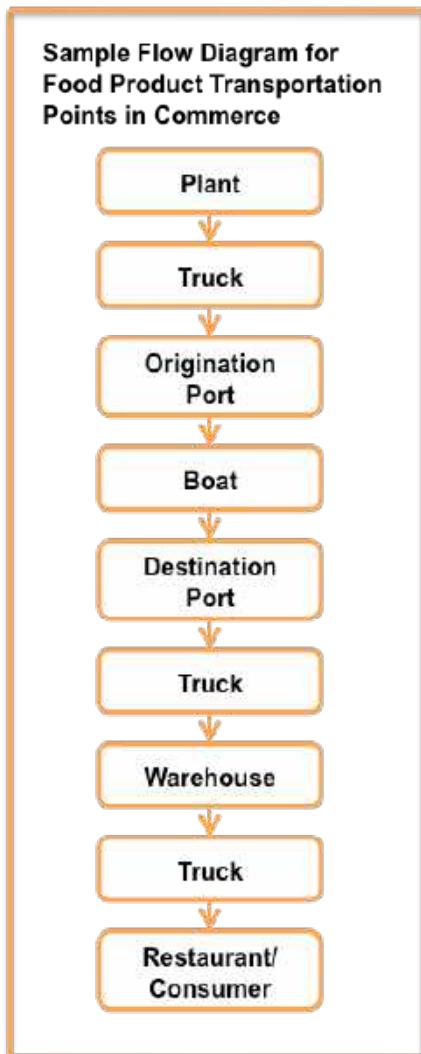
1. **Develop:** Identify vulnerable points where intentional contamination could occur and write a plan to minimize risk.
2. **Implement:** Implement necessary security measures at points identified in the assessment.
3. **Test:** Periodically test the plan using simple measures, such as checking locked doors or making unannounced perimeter checks, and document your actions using a form. Not all security measures need to be tested at the same frequency.
4. **Review and Maintain:** Review the plan at least annually, revising the plan as needed and taking appropriate actions.

The remainder of this guidance document includes additional information to assist you in developing your functional food defense plan.



1. Develop a Food Defense Plan

- ❖ Develop a flow diagram from your point-of-origin to final destination, including all shipping modes/routes. (See sample flow diagram below.)



- ❖ Identify all points of vulnerability where intentional contamination of the product could occur during the transportation and distribution process.
- ❖ Some of the information you will use to create your food defense plan may already exist in other documents, such as emergency response procedures. Make sure to consult these documents for information. There is no need to “reinvent the wheel” when developing your food defense plan.
- ❖ In the event of a threat to the food and food transportation sector or an elevated Homeland Security threat level specific to the food sector, identify any additional actions that are warranted.
- ❖ Determine what security measures should be implemented to minimize the risk at the vulnerable points identified. (You may already have some or all appropriate measures in place.)
- ❖ Write a comprehensive food defense plan.

- ◆ Key elements of a food defense plan should address:
 - Δ Inside security,
 - Δ Outside security,
 - Δ Storage security,
 - Δ Shipping and receiving security,
 - Δ Personnel security,
 - Δ Emergency response procedures, and
 - Δ Driver responsibilities and procedures.

2. **Implement Measures**

- ❖ Implement identified security measures at each point to ensure the protection of products from the time of shipment through delivery to each destination.
- ❖ Verify that contracted transporters (e.g., air, ground, maritime, rail) and storage/warehouse facilities have an effective food defense plan in effect. Consider including specific security measures in contracts and verify that measures are being met.
- ❖ FSIS has also created an easy-to-use online Food Defense Risk Mitigation Tool to assist with determining appropriate countermeasures which can be accessed at www.fsis.usda.gov.

3. **Test**

- ❖ Conduct drills regularly to test and verify the effectiveness of the plan. (A test can be as simple as checking door locks and access restriction procedures.)

4. **Review and Maintain**

- ❖ Periodically review policies and procedures in the plan and update as necessary. Document actions taken.

For Resources and More Information

If you have questions or need clarification about these guidelines, contact FSIS' Policy Development Division at 1-800-233-3935 or the Small Plant Help Desk at 1-877-FSIS-HELP (1-877-374-7435).

To obtain additional copies of these guidelines, visit FSIS' Web site at: www.fsis.usda.gov, or call 1-877-374-7435. The Web site also includes additional food defense guidance on:

- *Food Defense Plans,*
- *Food defense audio and video podcasts,*
- *A Food Defense Risk Mitigation Tool, and*
- *Warehouse and distributions centers.*

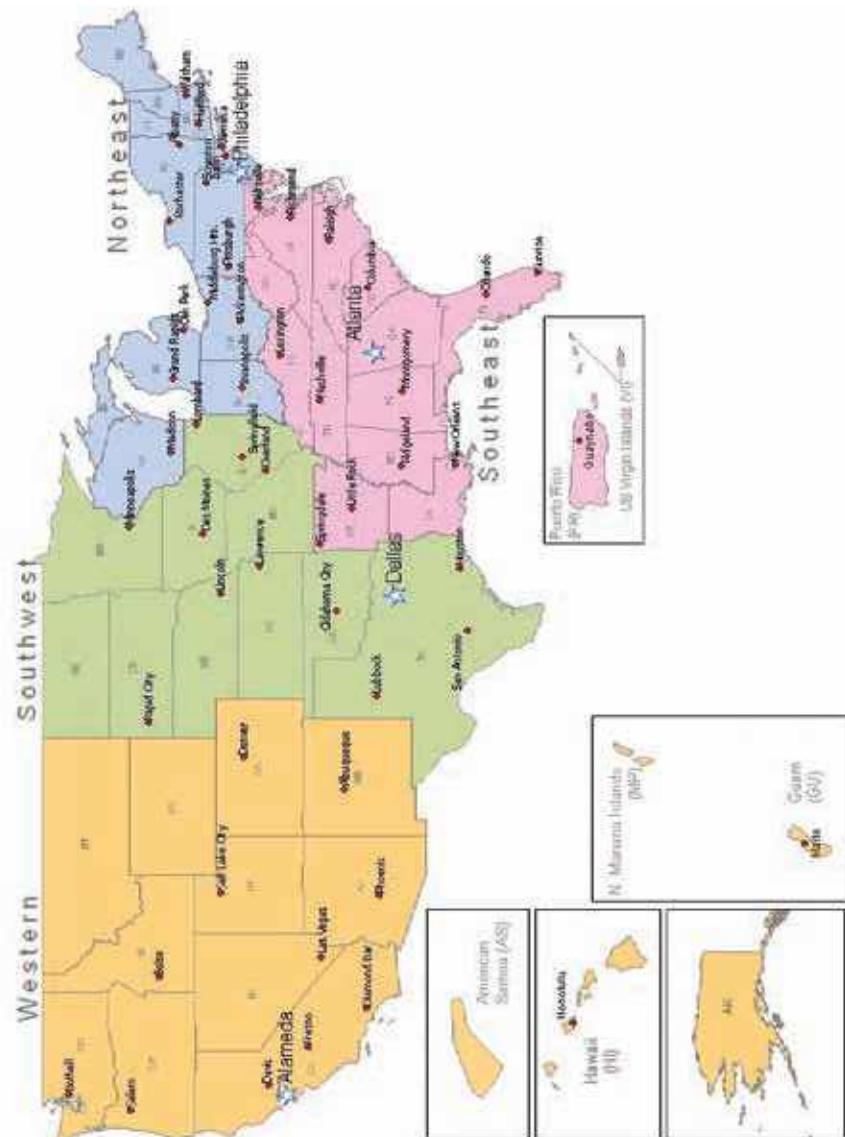
Some information is also available in Spanish, Vietnamese, Chinese, and Korean.

Further information on the safe and secure transportation of food is available from:

- *Transportation Security Administration: www.tsa.gov/what_we_do*
- *Food and Drug Administration: www.fda.gov/Food/FoodDefense/default.htm*
- *U.S. Postal Service: www.usps.com/cpim/ftp/pubs/pub166/*
- *U.S. Customs and Border Protection: www.cbp.gov/xp/cgov/trade/cargo_security/*
- *Customs Trade Partnership Against Terrorism (C-TPAT): www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/what_ctpat/ctpat_overview.xml*
- *First Observer Program: www.FirstObserver.com*
- *American Trucking Association: www.truckline.com/AdvIssues/security/Pages*
- *USDA-Office of the Inspector General (local contacts): www.usda.gov/oig/national.htm*
- *FBI Local Weapons of Mass Destruction Coordinator Contacts: www.fbi.gov/contact-us*
- *Owner Operator Independent Drivers Association (OOIDA): www.oida.com*

Funding resources may be available to enhance your security program through the Department of Homeland Security (DHS) grant office at www.grants.gov.

FSIS
Office of Investigation, Enforcement and Audit
Regional Offices



How to Contact FSIS

Office of Investigation, Enforcement and Audit

Regional Offices

Western Region

620 Central Avenue
Building 2 B, 2nd Floor
Alameda, CA 94501
(510) 769-5700

Alaska, American Samoa, Arizona,
California, Colorado, Guam, Hawaii,
Idaho, Montana, Mariana Islands,
Nevada, New Mexico, Oregon, Utah,
Washington, Wyoming

Southwest Region

1100 Commerce Street, Room 557
Dallas, TX 75242
(214) 767-9101

Illinois, Iowa, Kansas, Minnesota,
Missouri, Nebraska, North Dakota,
Oklahoma, South Dakota, Texas

Southeast Region

100 Alabama Street, SW
1924 Building, Suite 3R95
Atlanta, GA 30303
(404) 562-5962

Alabama, Arkansas, Delaware, District
of Columbia, Florida, Georgia,
Kentucky, Louisiana, Maryland,
Mississippi, North Carolina, Puerto
Rico, South Carolina, Tennessee,
Virgin Islands, Virginia, West Virginia

Northeast Region

Mellon Independence Center
701 Market Street, Suite 4100 C
Philadelphia, PA 19106
(215) 597-4219

Connecticut, Maine, Massachusetts,
Michigan, Indiana, New Hampshire,
New Jersey, New York, Ohio,
Pennsylvania, Rhode Island, Vermont,
Wisconsin



USDA is an equal opportunity provider and employer.