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

# FSIS DIRECTIVE	5420.3, Revision 5	6/25/08

HOMELAND SECURITY THREAT CONDITION RESPONSE – SURVEILLANCE OF ESTABLISHMENTS AND PRODUCTS IN COMMERCE

I. PURPOSE

A. This directive describes the procedures that Food Safety and Inspection Service (FSIS), Office of Program Evaluation, Enforcement and Review (OPEER), Compliance and Investigations Division (CID), personnel will follow at in-commerce facilities and ports-of-entry (non-official establishment) when the Department of Homeland Security declares a threat condition Yellow, Orange, or Red.

Key Points Covered

- establishes how threat condition declarations are to be communicated to CID personnel;

- provides specific instructions to CID personnel on how to respond to threat condition declarations;

- provides procedures to implement food defense surveillance procedures and effectively address and resolve noted security concerns in order to ensure that food in commerce is protected, thereby protecting pubic health;

- provides instructions for the CID personnel when checking to see if an establishment has a food defense plan.

C. If there is an actual terrorist attack on an in-commerce facility or port-of- entry that handles FSIS-regulated products, OPEER-CID Investigators will take immediate precautions to ensure their personal safety and to notify appropriate law enforcement officials, their immediate supervisor, and the Assistant Administrator (AA) of OPEER. In addition, the OPEER AA may request the activation of the FSIS Emergency Management Committee (EMC) through the Non-Routine Incident Management System (see FSIS Directive 5500.2, Non-Routine Incident Response).

II. CANCELLATION

FSIS Directive 5420.3, Revision 4, Homeland Security Threat Condition Response – Food Defense Verification Procedures, dated 10/31/06.

III. REASON FOR REISSUANCE

FSIS is reissuing this directive in its entirety to incorporate instructions related to documentation of food defense surveillance findings the In-Commerce System (ICS) and to advise that the SharePoint site has been discontinued. This issuance also will clarify the frequency for conducting food defense surveillance procedures and describe how the data generated from the procedures will be used.

IV. REFERENCES

9 CFR part 300 to end
FSIS Directive 5420.1, Revision 4, Homeland Security Threat Condition Response – Food Defense Verification Procedures
FSIS Directive 5420.4, Revision 4, Homeland Security Threat Condition Response – Emergency Procedures for the Office of International Affairs Import Inspection Division
FSIS Directive 5500.2, Non-Routine Incident Response
Homeland Security Presidential Directive/HSPD-9, Subject: Defense of United States Agriculture and Food
Public Health Security and Bioterrorism Act of 2002, Section 332 (21 USC 679C)

V. BACKGROUND

In 2002, the White House Office of Homeland Security established a Homeland Security Advisory System based on color. This System provides a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. A declaration of a Threat Condition Elevated (Yellow) by the Department of Homeland Security indicates that there is an elevated risk of terrorist attacks. A declaration of a Threat Condition High (Orange) indicates that there is a high risk of terrorist attacks. A declaration of a Threat Condition Severe (Red) reflects a severe risk of terrorist attacks. While the threat may or may not involve the nation's food supply, it is imperative that program personnel take certain immediate actions during such threat conditions to ensure the safety of meat, poultry, and egg products. Given what is required to respond to a credible threat of a terrorist attack, program personnel must clearly understand their roles, and what will be required of them to respond properly to that threat.

VI. NOTIFICATION

A. In the event of a declaration of any threat condition:

- Elevated (Yellow), when there is an elevated risk of terrorist attacks,
- High (Orange), when there is a high risk of terrorist attacks, or
- Severe (Red) when there is a severe risk of terrorist attacks,

by the Department of Homeland Security, FSIS' Office of Food Defense and Emergency Response (OFDER) will inform the FSIS Administrator and the FSIS Management Council. OFDER will issue an e-mail letter to all employees notifying them of the heightened threat condition.

B. CID headquarters will notify its personnel when the threat level changes from yellow to orange or red with no specific threat to the food and agriculture sector, in addition to the e-mail notification from OFDER. The CID Regional Offices, upon notification by CID headquarters of an elevated threat level, will:

1. Ensure that on-call procedures and updated personnel contact information are in place and ready for activation; and

2. Direct Investigators to inform management of in-commerce facilities or ports-of-entry, visited during the course of their duties of the current threat level.

C. OFDER will communicate the downgrading of a threat condition to CID personnel through the senior executive leadership in OPEER.

VII. SPECIFIC THREAT CONDITION ACTIVITIES

The following are the actions to take in the event of a declaration of:

A. Threat Condition Elevated (Yellow), High (Orange) or Severe (Red) with no specific threat to the food and agricultural sector

1. When the threat condition is elevated (Yellow), high (Orange), or severe (Red) with no specific threat to the food and agriculture section, investigators will conduct Food Defense Verification Procedures listed in Section IX.

2. Notify management of in-commerce facilities or ports-of-entry about the change of the alert status.

B. Threat Condition High (Orange) with a specific threat to the food and agricultural sector

1. CID headquarters managers and Regional Offices will be placed in a 24/7 on-call status.

2. CID Regional Offices, upon notification by CID headquarters of the threat level, will:

a. direct Investigators to perform applicable Food Defense Surveillance Procedures described in Section IX at in-commerce facilities and ports-of-entry;

b. place CID Supervisory Investigators in a 24/7 on-call status;

c. direct the collection of product samples as needed; and

d. coordinate activity at ports of entry with Office of International Affairs (OIA) personnel.

C. Threat Condition Severe (Red) with a specific threat to the food and agricultural sector

Investigators are to conduct procedures listed above under Threat Condition High (Orange) with a specific threat to the food and agricultural sector and the CID Regional Offices will:

a. place all field personnel in a 24/7 on-call status; and

b. instruct Investigators to carry out any additional activities as directed by CID headquarters, OPEER management, through emergency response issuances, or by incident command.

VIII. FOOD DEFENSE PLAN

A. Although not required by FSIS statute or regulation, FSIS has urged management at in-commerce facilities and ports-of-entry to develop functional food defense plans to set out control measures to prevent intentional adulteration of product. FSIS considers these plans to be important preparatory measures. The plan should be developed, written, implemented, assessed, and maintained if it is to be functional. The Agency has developed guidance materials to assist in the development and understanding of what constitutes a food defense plan for warehouses and distribution centers. They are available on the FSIS web site at: *http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Guidance_Materials/index.asp.*

B. Management at in-commerce facilities or ports-of-entry is not obligated to share a copy of its written plan with Investigators. If the food defense plan is shared, Investigators should only use the plan to help them readily identify how management has addressed food defense. If management is not implementing elements of its plan, Investigators cannot take action on that fact because there are not requirements for such plans. Investigators are not to show or share the plan with any outside source because it may contain sensitive security information.

NOTE: When establishment management develops and implements a new food defense plan, or when management revises an existing food defense plan, Investigators are to reference this under Block 9 of FSIS Form 5420-3 when they re-visit the facility or port-of-entry.

IX. FOOD DEFENSE SURVEILLANCE PROCEDURES

A. CID Investigators conduct surveillance reviews in accordance with FSIS Directive 8010.1, Methodology for Conducting In-Commerce Surveillance Activities, at warehouses, distributors, and other in-commerce facilities and at ports-of-entry to verify that persons and firms, whose business activities involve FSIS-regulated products, prepare, store, transport, sell, or offer for sale or transportation such products in compliance with FSIS statutory and regulatory requirements. These surveillance reviews include procedures for food defense surveillance as well as for food safety, imported products, and other in-commerce surveillance activities.

B. CID Investigators conduct food defense surveillance procedures to identify potential security vulnerabilities at in-commerce facilities and ports-of-entry that increase the risk of intentionally adulterated meat, poultry, and egg products. A potential vulnerability can be any part of the food continuum system identified at the facility or port-of-entry where measures can be taken to protect food products from intentional product tampering and adulteration. Examples of potential vulnerabilities include:

- Unrestricted access to product storage and staging areas;
- Unrestricted to product processing areas;
- Unrestricted access to shipping/receiving areas; or
- Unrestricted access to water systems.

C. When Investigators conduct food defense surveillance procedures, they will:

1. Food Defense Plan – determine whether the facility or port-of-entry has:

a. a written food defense plan that consists of standard operating procedures for preventing intentional product tampering and adulteration; and

b. contact information (e.g., police, state and local health agencies) to be used if product is intentionally adulterated.

2. Outside Security – determine whether the facility or port-of-entry has a means to protect the outer perimeter, such as a surveillance system (e.g., cameras, security guards, lighting, alarm system, locks) to secure the facility and outside premises.

3. Inside Security –determine whether the facility or port-of-entry has:

a. a surveillance system (e.g., cameras, security guards, lighting, alarm system, locks) to secure the inside premises;

b. measures in place to ensure that all persons (e.g., employees, contractors, construction or maintenance personnel) in the facility or port-of-entry are authorized, properly identified, and restricted from areas as appropriate;

c. a process for the use, storage and controlled access of hazardous materials in the facility or port-of-entry to prevent product adulteration; and

d. a process to protect food and/or food ingredients, including water used in products prepared by the facility or port-of-entry, especially if it is well water.

NOTE: This question applies to facilities that only store product (e.g., distributors and warehouses AND to facilities that process products (e.g.; retail stores and restaurants).

4. Receiving/Shipping –determine whether the facility or port-of-entry has:

a. a process that restricts access to the receiving/shipping areas to authorized personnel;

b. a process to verify that incoming/shipped products are consistent with shipping documents;

c. a process to examine all incoming products for indications of apparent tampering or adulteration (e.g., opened or resealed boxes, the presence of an unidentified substance on packaging or product, or questionable products, packaging or labeling); and

d. a process for maintaining security of products during loading/shipping, (e.g., trucks and trailers are locked or sealed while not under the direct supervision of company personnel).

5. Product Observation – determine whether there are any indications for products currently held in storage by the facility or port-of-entry of apparent product tampering or adulteration.

D. CID Investigators will conduct food defense surveillance procedures when a facility or port-of-entry is reviewed for the first time or during a follow-up surveillance review where food defense surveillance procedures were not conducted within the previous 12 months.

X. FOOD DEFENSE SURVEILLANCE PROCEDURE DOCUMENTATION

A. Investigators will conduct the food defense surveillance procedures listed in paragraph IX above at threat condition Elevated (Yellow) or higher and will document the findings in the ICS.

B. If Investigators find food defense vulnerabilities, they are to provide a hard copy of the completed FSIS Form 5420-3 to the management at the time of the visit or subsequently via fax or regular mail.

NOTE: FSIS Form 5420-3 should be completed and printed using the ICS. The form can also be found in Outlook:\\Public Folders\All Public Folders\Agency Issuances\Forms\FSIS 5,000 Series.

C. Investigators may not have access to ICS while conducting the food defense surveillance procedures. Investigators are to document findings on FSIS Form 5420-3 and enter the information from the Form into ICS as soon as possible.

D. CID supervisors and managers, as well as other OPEER and OFDER personnel, will have access to the data entered by Investigators, in addition to having access to summary reports of the data in the ICS application.

XI. ADULTERATED PRODUCT OR POSSIBLE TAMPERING

A. Investigators are to immediately follow the established policy described in FSIS Directive 8410.1, Detention and Seizure, when they have reason to believe that meat, poultry, or egg products in commerce are adulterated, misbranded, or otherwise in violation of the Federal Meat Inspection Act (21 U.S.C. 672), Poultry Products Inspection Act (21 U.S.C. 467a) or the Egg Products Inspection Act (21 U.S.C. 1048).

B. Investigators are to follow procedures defined in FSIS Directive 5500.2, Non-Routine Incident Response, when they have evidence or information that indicates that

product may have been tampered with or other findings that require completing an NRIR.

C. The Regional Manager will determine whether he or she should refer the information obtained regarding possible tampering to the Office of the Inspector General (OIG) for investigation using the criteria in the Memorandum of Understanding with OIG.

XII. ANALYSIS OF THE DATA

OFDER will analyze the food defense surveillance procedure information submitted to the ICS system on a monthly basis. The data will be analyzed for trends that would lead to improvements in food defense guidance or vulnerability weaknesses. The analysis will also identify positive trends that can be shared with all agri-business stakeholders. OFDER will collaborate with OPEER and OIA if further analyses are needed.

Direct all questions on this directive through supervisory channels.

Assistant Administrator
Office of Policy and Program Development