

UNITED STATES DEPARTMENT OF AGRICULTURE  
FOOD SAFETY AND INSPECTION SERVICE

WASHINGTON, DC

---

---

# FSIS DIRECTIVE

5420.3  
Revision 6

8/1/11

---

---

**FOOD DEFENSE SURVEILLANCE PROCEDURES AND  
NATIONAL TERRORISM ADVISORY SYSTEM ALERT RESPONSE  
FOR THE OFFICE OF PROGRAM EVALUATION, ENFORCEMENT AND REVIEW**

## I. PURPOSE

A. This directive describes the Food Defense Surveillance Procedures that Food Safety and Inspection Service (FSIS), Office of Program Evaluation, Enforcement and Review (OPEER), Compliance and Investigations Division (CID) personnel are to perform and the frequency with which these procedures are to be performed. This directive also describes additional actions that are to be followed at in-commerce facilities and facilities (other than official import inspection establishments) located at ports-of-entry (“facilities”) when the Department of Homeland Security (DHS) issues a National Terrorism Advisory System (NTAS) alert.

B. On January 27, 2011, the DHS announced that it would discontinue the color-coded Threat Conditions of the Homeland Security Advisory System (HSAS), on April 27, 2011, in favor of a new system, the NTAS.

C. If there is an actual terrorist attack on a facility, OPEER CID Investigators will take immediate precautions to ensure their personal safety and to notify appropriate law enforcement officials, their immediate supervisor, and the OPEER Assistant Administrator (AA). In addition, the OPEER senior executive leadership may request the activation of the FSIS Emergency Management Committee (EMC) (see FSIS Directive 5500.2, Significant Incident Response).

### *KEY POINTS:*

- *How NTAS alerts are to be communicated*
- *How to record any findings and respond to NTAS alerts*
- *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 public health*
- *How to determine if a facility has a functional food defense plan*

## **II. CANCELLATION**

FSIS Directive 5420.3, Revision 5, Homeland Security Threat Condition Response – Surveillance of Establishments and Products In Commerce, dated 06/25/08

## **III. REASON FOR REISSUANCE**

FSIS is reissuing this directive to reflect the DHS's NTAS, which replaced the color-coded Threat Conditions of the HSAS.

## **IV. REFERENCES**

9 CFR Part 300 to end

FSIS Directive 5420.1, Food Defense Verification Procedures and National Terrorism Advisory System Alert Response for the Office of Field Operations

FSIS Directive 5420.4, Food Defense Verification and Surveillance Procedures and National Terrorism Advisory System Alert Response for the Office of International Affairs Import Inspection Division

FSIS Directive 5500.2, Significant Incident Response

FSIS Directive 8010.1, Methodology for Conducting In-Commerce Surveillance Activities

FSIS Directive 8410.1, Detention and Seizure

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**

A. Food defense is the protection of food products from intentional adulteration with chemical, biological, physical, or radiological agents. Food defense is an integral part of FSIS's mission of ensuring that the nation's commercial supply of meat, poultry, and processed egg products is safe, wholesome, and correctly labeled and packaged.

B. CID personnel conduct food defense surveillance tasks to identify potential vulnerabilities in facilities that could lead to or allow deliberate contamination.

C. When the Federal government receives information about a specific or credible terrorist threat to food or agriculture, additional actions may be needed to reduce the threat of intentional adulteration of food products. Given what is required to respond to a credible threat of a terrorist attack, Investigators must clearly understand their roles and what will be required of them to respond properly to that threat.

D. Under the new 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. These alerts include a clear statement that there is an "imminent threat" or "elevated threat." The alerts also provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses, and governments can

take.

E. The NTAS alerts are based on the nature of the threat. In some cases, alerts are sent directly to law enforcement or affected areas of the private sector, while in others, alerts are issued more broadly to the American people through both official and media channels—including a designated DHS webpage ([www.dhs.gov/alerts](http://www.dhs.gov/alerts)), as well as social media tools, including Facebook and Twitter (@NTASAlerts).

F. 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.

## **VI. NOTIFICATION**

A. If DHS issues an NTAS alert, the FSIS Office of Data Integration and Food Protection (ODIFP) Assistant Administrator (AA) or designee will determine whether the alert affects food or agriculture and, if so, will inform the FSIS Administrator and the FSIS Management Council. The ODIFP AA or designee will determine the appropriate distribution of the NTAS alert information, and will coordinate with the FSIS Office of Public Affairs and Consumer Education (OPACE) and the other program area AAs or their designees to notify employees, stakeholders, and the public, as appropriate. In the case of a significant incident, the FSIS Emergency Management Committee may be alerted or activated and other response actions taken pursuant to Directive 5500.2.

B. When notified regarding an NTAS alert, the CID Director will notify CID personnel (in addition to any notification by ODIFP or OPACE). The CID Regional Offices, upon notification by the Office of the Director 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, while at a facility, to inform the management of the current alert.

C. When an NTAS alert ends, ODIFP will notify the FSIS Administrator and the FSIS Management Council. ODIFP will coordinate with OPACE to notify employees, stakeholders, and the public, as appropriate.

## **VII. FOOD DEFENSE ACTIVITIES**

A. When there are no active NTAS alerts, or when the active alerts do not threaten food or agriculture:

1. Investigators are to conduct Food Defense Surveillance Procedures described in Section IX.

B. When there is an NTAS alert with elevated threat to food or agriculture:

1. The CID Director, CID headquarters staff, and CID Regional Offices will be placed in a 24/7 on-call status.
  2. CID Regional Offices, when notified by the CID Director of the threat level, are to:
    - a. Direct Investigators to perform Food Defense Surveillance Procedures described in Section IX;
    - b. Place CID Supervisory Investigators in a 24/7 on-call status;
    - c. Direct the collection of product samples as needed;
    - d. Coordinate with the Office of Public Health Science (OPHS) for testing of samples by the FSIS field laboratories or the Food Emergency Response Network (FERN); and
    - e. Coordinate activity at ports of entry with Office of International Affairs (OIA) personnel.
  3. Investigators, after being notified by the Regional Office of an elevated threat to food or agriculture, are to:
    - a. Conduct Food Defense Surveillance Procedures listed in Section IX; and
    - b. Inform management of facilities visited during the course of their duties of the current NTAS alert.
- C. When there is an NTAS alert with imminent threat to food or agriculture:
1. CID Regional Offices are to:
    - a. Place all Investigators 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.
  2. After being notified by the Regional Office of an imminent threat to food or agriculture, Investigators are to:
    - a. Conduct procedures listed above under Section VII B (NTAS alert with elevated threat to food or agriculture); and
    - b. Conduct any additional activities as directed by CID headquarters, OPEER management, through emergency response issuances, or by incident command.

## **VIII. FOOD DEFENSE PLAN**

A. FSIS has urged management at facilities to develop functional food defense plans that set out control measures to prevent intentional adulteration of product. Although a functional food defense plan is not required, FSIS considers these plans to be important preparatory measures. 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, and the plan is reviewed at least annually and revised if needed. The Agency has developed guidelines on the food defense plans, which are available on the FSIS Web site at:

[http://www.fsis.usda.gov/Food\\_Defense\\_&\\_Emergency\\_Response/Guidance\\_Materials/index.asp](http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Guidance_Materials/index.asp).

B. 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.

## **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 facilities located 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 facilities that increase the risk of intentional product tampering and adulteration of meat, poultry, and egg products. A potential vulnerability can be any part of the food continuum system identified at the facility where measures can be taken to protect food products from intentional product tampering and adulteration. Examples of potential vulnerabilities include:

1. Unrestricted access to product storage and staging areas;
2. Unrestricted access to product processing areas;
3. Unrestricted access to shipping/receiving areas; or
4. Unrestricted access to water systems.

C. When Investigators conduct Food Defense Surveillance Procedures, they are to:

1. Determine whether the facility has a written food defense plan that consists of standard operating procedures for preventing intentional product tampering and adulteration; and contact information (e.g., for police, and state and local health

agencies) to be used if product is intentionally adulterated;

2. Determine whether the facility has a means to protect the outer perimeter and outside premises of the facility (e.g., cameras, security guards, lighting, alarm system, and locks);
3. Observe and determine whether the facility has:
  - a. A surveillance system (e.g., cameras, security guards, lighting, and alarm system) to secure the inside premises;
  - b. Measures in place to ensure that all persons (e.g., employees, contractors, and construction or maintenance personnel) in the facility 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 to prevent product adulteration; and
  - d. A process to protect food or food ingredients, including water used in products prepared by the facility, especially if it is well water.

**NOTE:** This step applies to facilities that store products only (e.g., distributors and warehouses) and facilities that process products (e.g., retail stores and restaurants).

4. Observe and determine whether the facility 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. Determine whether there are any indications of apparent product tampering or adulteration of products currently held in storage by the facility.

D. CID Investigators are to conduct Food Defense Surveillance Procedures when a facility is reviewed for the first time or during a follow-up surveillance review where Food Defense Surveillance Procedures have not been conducted within the previous 12 months.

## **X. FOOD DEFENSE SURVEILLANCE PROCEDURE DOCUMENTATION**

A. Investigators are to conduct the Food Defense Surveillance Procedures listed in section IX above and will document the findings in the In-Commerce System (ICS).

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

**NOTE:** Investigators are to complete FSIS Form 5420-3 and print it using ICS. The form can also be found at:

<https://inside.fsis.usda.gov/fsis/emp/static/global/forms/forms.jsp>.

C. If Investigators do not have access to ICS while conducting the Food Defense Surveillance Procedures, they 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, as well as other OPEER and designated ODIFP 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 processed egg products in commerce are adulterated, misbranded, or otherwise in violation of the Federal Meat Inspection Act, Poultry Products Inspection Act, or the Egg Products Inspection Act.

B. Investigators are to follow procedures defined in FSIS Directive 5500.2, Significant Incident Response, when they have evidence or information that indicates that product may have been tampered with or other findings that may require completion of an Incident Report (IR).

C. The Regional Directors 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. DATA ANALYSIS**

On at least an annual basis, the Data Analysis and Integration Group (DAIG) within ODIFP is to review food defense verification and surveillance activity data to evaluate the overall frequency and number of food defense procedures performed by Investigators, as well as potential trends in food defense vulnerabilities or concerns. The analyses will inform future guidance and policy regarding performance of food defense surveillance activities. At least annually, ODIFP will provide a summary of this analysis to the OPEER AA. ODIFP will collaborate with OPEER and OIA if further analyses are needed.

Refer questions regarding this directive to the Policy Development Division through askFSIS at <http://askfsis.custhelp.com> or by telephone at 1-800-233-3935.

A handwritten signature in black ink, appearing to read "David Joseph". The signature is written in a cursive style with a prominent initial "D".

Assistant Administrator  
Office of Policy and Program Development