

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

FSIS DIRECTIVE

5420.3
Rev. 7

2/6/14

**FOOD DEFENSE SURVEILLANCE PROCEDURES
AND NATIONAL TERRORISM ADVISORY SYSTEM ALERT RESPONSE
FOR THE OFFICE OF INVESTIGATION, ENFORCEMENT AND AUDIT**

I. PURPOSE

A. This directive describes the Food Defense Surveillance Procedures that Food Safety and Inspection Service (FSIS), Office of Investigation, Enforcement and Audit (OIEA), 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. If there is an actual terrorist attack on a facility, OIEA personnel are to take immediate precautions to protect their personal safety and to notify appropriate law enforcement officials, their immediate supervisor, and the OIEA Assistant Administrator (AA) of the situation. In addition, the OIEA senior executive leadership may request the activation of the FSIS Emergency Management Committee (EMC) (see [FSIS Directive 5500.2](#), *Significant Incident Response*).

C. FSIS is reissuing this directive as result of the Agency's reorganization and of the change in the name of the office to OIEA from the Office of Program, Evaluation, Enforcement, and Review.

KEY POINTS:

- *How NTAS alerts are to be communicated*
- *How to respond to NTAS alerts*
- *How to effectively address and resolve noted security concerns to ensure that food that is in commerce is protected, thereby protecting public health*
- *How to determine whether a facility has a functional food defense plan (FDP)*

II. CANCELLATION

FSIS Directive 5420.3, Revision 6, Food Defense Surveillance Procedures and National Terrorism Advisory System Alert Response for the Office of Program Evaluation, Enforcement, and Review, dated 08/01/11

III. BACKGROUND

A. Food defense is the protection of food products from intentional adulteration with chemical, biological, physical, or radiological agents.

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.

D. Under NTAS, 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” (warns of a credible, specific, and impending terrorist threat against the United States) or an “elevated threat” (warns of a credible terrorist threat against the United States). 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.

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 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.

G. The Agency has developed numerous food defense guidance documents (e.g., model food defense plans, worksheets, checklists, and fact sheets) for consumers, industry, and state and local agencies. All of these materials are available on the FSIS Website at [Food Defense and Emergency Response](#).

IV. NTAS ALERT NOTIFICATION

A. The FSIS Office of Data Integration and Food Protection (ODIFP) AA or designee is to determine whether the NTAS alert is expected to affect food or agriculture.

1. If the threat is expected to affect food or agriculture, the AA or the designee is to inform the FSIS Administrator and FSIS Management Council.
2. The ODIFP AA or designee is to determine the appropriate distribution of the NTAS alert information and to coordinate with the FSIS Office of Public Affairs and Consumer Education (OPACE), and OIEA to notify employees, stakeholders, and the public, as appropriate.
3. 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](#).

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 CID Director of the NTAS alert, to:

1. Ensure that on-call procedures and updated personnel contact information are in place and ready for activation; and
2. Direct CID personnel, while at a facility, to inform the management of the alert.

C. When an NTAS alert ends, ODIFP is to notify the FSIS Administrator and the FSIS Management Council. ODIFP is to coordinate with OPACE and OIEA, to notify employees, stakeholders, and the public, as appropriate. The CID Regional Offices, upon notification by the CID Director that an alert has ended, is to direct CID personnel, while at a facility, to inform facility management of the change in NTAS alert status.

V. FOOD DEFENSE ACTIVITIES

A. When there are no active NTAS alerts, or when the active alerts do not threaten food or agriculture, CID personnel are to conduct Food Defense Surveillance Procedures described in Section VII.

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 are to 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 CID personnel to perform Food Defense Surveillance Procedures described in Section VII;
 - 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 Field Operations (OFO) personnel.
3. CID personnel, 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 VII; 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 field personnel in a 24/7 on-call status; and
 - b. Instruct personnel to carry out any additional activities as directed by CID headquarters, OIEA 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, CID personnel are to:
 - a. Conduct procedures listed above under Section V B (NTAS alert with elevated threat to food or agriculture); and

- b. Conduct any additional activities as directed by CID headquarters, OIEA management, through emergency response issuances, or by incident command.

VI. FUNCTIONAL FOOD DEFENSE PLAN

A. The development of a FDP is voluntary. In-commerce facilities are not required to develop a functional FDP, and they are not required to share the plan they have developed with the CID personnel.

B. If the inspected facility has developed a FDP, CID personnel are to determine whether the plan is functional. A functional FDP has all of the following characteristics:

1. The plan is written;
2. The plan includes but is not limited to measures that address: outside security (e.g., door locks); inside security (e.g., restricted ingredients are secured); personnel security (e.g., method to identify employees in the facility); and incident response security (e.g., procedures to report unusual activities);
3. The plan is reviewed annually (i.e., within the prior 12 months) and revised when changes occur in the facility that might affect the vulnerability of product; and
4. The measures are tested annually (this testing can be as simple as testing locks on doors and conducting a periodic perimeter search).

C. When facility management develops and implements a new food defense plan, or when management revises an existing food defense plan, CID personnel are to reference this fact under Block 6 of FSIS Form 5420-3 when they re-visit the facility.

VII. FOOD DEFENSE SURVEILLANCE PROCEDURES

A. CID personnel conduct surveillance activities in accordance with [FSIS Directive 8010.1](#), *Methodology for Conducting In-Commerce Surveillance Activities*, at warehouses, distributors, and other in-commerce facilities and facilities (other than official import inspection establishments) 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 activities include procedures for food defense surveillance as well as for food safety, imported products, and other in-commerce surveillance activities.

B. CID personnel conduct Food Defense Surveillance Procedures to identify potential security vulnerabilities at facilities that could 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 should be taken to protect food products from intentional product tampering and adulteration, but such a measure is found to be missing or not in place. 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 CID personnel conduct Food Defense Surveillance Procedures, they are to:

1. Determine whether the facility has a functional food defense plan;
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 of, storage of, 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 is to be taken in 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 personnel 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.

VIII. FOOD DEFENSE SURVEILLANCE PROCEDURE DOCUMENTATION

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

B. If CID personnel 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: CID personnel are to complete FSIS Form 5420-3 and print it using ICS.

C. If CID personnel 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 OIEA and designated ODIFP personnel, will have access to the data entered by CID personnel, in addition to having access to summary reports of the data in the ICS application.

IX. ADULTERATED PRODUCT OR POSSIBLE TAMPERING

A. CID personnel 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. CID personnel are to follow procedures defined in [FSIS Directive 5500.2](#) 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.

X. DATA ANALYSIS

ODIFP is to annually review food defense verification and surveillance activity data to evaluate the overall frequency and number of food defense procedures performed by CID personnel as well as potential trends in food defense vulnerabilities or concerns. The analyses will assist in the development of future guidance and policy regarding performance of food defense surveillance activities. At least annually, ODIFP will provide a summary of this analysis to the OIEA AA.

XI. QUESTIONS

Refer questions regarding this directive through supervisory channels.



Assistant Administrator
Office of Policy and Program Development