

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

| | | |
|-----------------------|-----------------------|----------|
| FSIS DIRECTIVE | 5420.3, Revision 4 | 10/31/06 |
|-----------------------|-----------------------|----------|

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

I. PURPOSE

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

- food defense surveillance procedures to aid in the detection of possible vulnerabilities to meat, poultry, and egg products in commerce;
- a mechanism to document findings of food defense surveillance procedures; and
- the method for communicating elevated threat conditions within FSIS, and how CID personnel will respond to elevated threat conditions.

B. If there is an actual terrorist attack on a firm that handles product in commerce, OPEER personnel will take immediate measures to ensure the safety of any affected FSIS personnel and will notify appropriate law enforcement officials and the Assistant Administrator of OPEER.

II. CANCELLATION

FSIS Directive 5420.3, Revision 3, dated 9/14/06

DISTRIBUTION: Inspection Offices; T/A Inspectors; TRA;
TSC; Import Offices

OPI: OPPEd

III. REASON FOR REISSUANCE

On September 15, 2006, FSIS issued revision 3 of this directive and on September 16, 2006, FSIS postponed the effective date to provide for the completion of training. Therefore, FSIS is reissuing this directive in its entirety to:

- update food defense procedures at or above a threat condition “Elevated” (Yellow) level; and
- make available FSIS Form 5420-3, Food Defense Surveillance Findings.

IV. REFERENCES

9 CFR part 300 to end
FSIS Directive 5420.1, Revision 3, Homeland Security Threat Condition Response – Food Defense Verification Procedures
FSIS Directive 5500.2, Non-Routine Incident Response

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 the 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 the firms 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. FOOD DEFENSE SURVEILLANCE PROCEDURES

The purpose of the following food defense surveillance procedures is to identify potential vulnerabilities in the security at a firm. A potential vulnerability can be at any location in the firm where the possibility of deliberate product contamination can occur and reasonable measures can be taken to prevent the occurrence. Examples of potential vulnerabilities include unlocked gates, insufficient lighting of outside premises and no restricted access for non-employees.

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

Investigators will conduct the following food defense surveillance procedures:

1. Food Defense Plan – determine whether the firm (e.g., warehouse, distribution center) has the following:
 - a. a written food defense plan that consists of standard operating procedures for preventing intentional product tampering and adulteration; and
 - b. contact information to be used if product is intentionally adulterated, e.g., police, state and local health agencies.

2. Outside Security – determine whether the firm has a surveillance system (e.g., cameras, security guards, lighting, alarm system, locks) to secure the outside premises and the firm.

3. Inside Security – determine whether the firm 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 in the firm (e.g., employees, contractors, construction or maintenance personnel) are authorized, properly identified, and restricted from areas as appropriate;

c. a process for the use and storage of hazardous materials in the firm to prevent adulteration; and

d. a process to protect food and food ingredients including the water used in products, especially if it is well water.

4. Receiving/Shipping – determine whether the firm 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 firm personnel).

5. Product Observation – Observe products currently held in storage by the firm to determine whether there are any indications of apparent product tampering or adulteration.

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

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

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

a. direct Investigators to perform the food defense surveillance procedures at firms based on vulnerabilities as identified by the Regional Office;

b. place CID field supervisors 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, emergency response issuances, or incident command.

VIII. FOOD DEFENSE SURVEILLANCE DOCUMENTATION

A. Investigators will conduct the food defense surveillance procedures listed in paragraph VII above at threat condition Elevated (Yellow) or higher and will document the findings in the intranet-based "Share Point" application.

B. Because Investigators may not have access to Share Point while conducting the food defense surveillance procedures, they may document findings on FSIS Form 5420-3. Investigators are to enter the information from the Form into Share Point as soon as practical.

C. When Investigators find a food defense vulnerability, they are to provide a typed copy of the completed FSIS Form 5420-3 to the firm at the time of the visit or subsequently via fax or regular mail.

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

IX. 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 or 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.

Direct all questions on this directive through supervisory channels.



Assistant Administrator
Office of Policy, Program, and Employee Development