

### **Prevent customer's access to critical areas of your facility.**

Prevent customer's access to food preparation and storage and dishwashing areas in the non-public areas of the establishment, including loading docks.

**R**

Could you provide **REPORTS** about the security of your products while under your control?

### **Periodically evaluate the effectiveness of your security management system.**

Review and verify, at least annually, the effectiveness of the security management program (for example, using knowledgeable in-house or third party staff to conduct tampering or other malicious, criminal, or terrorist action exercises and mock recalls and to challenge computer security systems), revising the program accordingly, and keeping this information confidential.

### **Perform random food defense inspections.**

Perform random food defense inspections of all appropriate areas of the facility (including receiving and warehousing, where applicable) using knowledgeable in-house or third party staff, and keeping this information confidential.

### **Establish and Maintain Records**

On December 9, 2004, FDA issued a final rule that requires the establishment and maintenance of records by persons who manufacture, process, pack, transport, distribute, receive, hold, or import food in the United States. Such records are to allow for the identification of the immediate previous sources and the immediate subsequent recipients of food. The

final rule implements Section 306 of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (See 69 FR 71562; December 9, 2004 (<http://www.cfsan.fda.gov/~dms/frrecord.html>)).

### **Evaluate lessons learned.**

Evaluate the lessons learned from past tampering or other malicious, criminal, or terrorist actions and threats.

**T**

What do you do and who do you notify if you have a **THREAT** or issue at your facility, including suspicious behavior?

### **Hold any product that you believe may have been affected.**

### **Contact the Food and Drug Administration**

If a food establishment operator suspects that any of his/her products that are regulated by the FDA have been subject to tampering, "counterfeiting," or other malicious, criminal, or terrorist action, FDA recommends that he/she notify the FDA 24-hour emergency number at 301-443-1240 or call their local FDA District Office.

FDA District Office telephone numbers are listed at: [http://www.fda.gov/ora/inspect\\_ref/iom/iomoradir.html](http://www.fda.gov/ora/inspect_ref/iom/iomoradir.html). FDA recommends that the operator also notify appropriate law enforcement and public health authorities.

**Additional ALERT information can be found at [www.cfsan.fda.gov/alert](http://www.cfsan.fda.gov/alert)**



# ALERT

## Questions & Answers

**The **ALERT** initiative is intended to raise the awareness of state and local government agency and industry representatives regarding food defense issues and preparedness. It is generic enough to apply to all aspects of the farm-to-table supply chain and is designed to spark thought and discussion with a variety of stakeholders. **ALERT** identifies five key points that industry and businesses can use to decrease the risk of intentional food contamination at their facility. This brochure provides additional background information in support of each letter of the **ALERT** acronym.**

# A

How do you **ASSURE** that the supplies and ingredients you use are from safe and secure sources?

## **Know your suppliers.**

Use only known, appropriately licensed or permitted (where applicable) contract manufacturing and packaging operators and sources for all incoming materials, including ingredients, compressed gas, packaging, labels, and materials for research and development.

## **Encourage your suppliers to practice food defense measures.**

Take reasonable steps to ensure that suppliers, contract operators and transporters practice appropriate food defense measures (for example, auditing, where practical, for compliance with food security measures that are contained in purchase and shipping contracts or letters of credit, or using a vendor approval program).

## **Request locked and/or sealed vehicles/containers/railcars.**

If sealed, obtain the seal number from the supplier and verify upon receipt, making arrangements to maintain the chain of custody when a seal is broken for inspection by a governmental agency or as a result of multiple deliveries.

## **Supervise off-loading of incoming materials.**

The supervision of incoming materials should pertain to deliveries that occur during normal business hours, as well as deliveries that occur during off hours.

# L

How do you **LOOK** after the security of the products and ingredients in your facility?

## **Implement a system for handling products.**

Have a system for receiving, storing, and handling distressed, damaged, returned, and rework products that minimizes their potential for being compromised or to compromise the security of other products (for example, destroying products that are unfit for human or animal consumption, products with illegible codes, products of questionable origin, and products returned by consumers to retail stores).

## **Track materials.**

Keep track of incoming materials and materials in use, including ingredients, compressed gas, packaging, labels, salvage products, rework products, and product returns.

## **Store product labels in a secure location and destroy outdated or discarded product labels.-**

## **Limit access and inspect facilities.**

Limit, to the extent possible, and conduct random inspections, on facilities such as, storage and handling facilities, vessels, vehicles, access to controls for airflow, water, electricity, and refrigeration.

## **Keep track of finished products.**

## **Encourage your warehousing operations to practice food defense measures.**

Ensure that public storage warehousing and shipping operations (vehicles and vessels) practice appropriate security measures (for example, auditing, where practical, for compliance with food security measures that are contained in contracts or letters of guarantee).

# E

What do you know about your **EMPLOYEES** and people coming in and out of your facility?

## **Conduct background checks on staff.**

Examine the background of all staff (including seasonal, temporary, contract, and volunteer staff, whether hired directly or through a recruitment firm) as appropriate to their position, considering candidates access to sensitive areas of the facility and the degree to which they will be supervised.

## **Know who belongs in your facility.**

Know who is and who should be on premises, and where they should be located, for each shift.

Provide an appropriate level of supervision to all staff, including cleaning and maintenance staff, contract workers, data entry computer support staff, and especially, new staff.

## **Establish an identification system for employees.**

Establish a system of positive identification and recognition that is appropriate to the nature of the workforce (for example, issuing uniforms, name tags, or photo identification badges with individual control numbers, color coded by area of authorized access), when appropriate.

## **Limit access by staff.**

Limit access so staff enter only those areas necessary for their job functions and only during appropriate work hours (for example, using key cards or keyed or cipher locks for entry to sensitive areas, or color coded uniforms).