

## FOODSERVICE DISTRIBUTION TOPICS

# **Operational Threat and Risk Assessment for the Foodservice Distribution Industry**



*Prepared by the*  
International Foodservice Distributors Association



**TABLE OF CONTENTS**

I. Introduction .....	1
II. Threats .....	2
III. Operational Risk Assessment and Procedures .....	3
General .....	3
People .....	3
Sourcing .....	4
Facilities .....	5
Systems .....	5
Transportation .....	6
IV. Response Actions .....	8

## I. INTRODUCTION

Quality control and anti-tampering measures developed by the food industry in cooperation with government agencies over the past two decades have made the U.S. food supply the safest in the world. Since the September 11 attacks, our industry has recognized that we must take additional proactive measures to ensure the safety of consumers. The safeguards that we developed to address long-standing food safety issues and past tampering incidents are being re-examined, strengthened and enforced with vigilance in light of these recent events.

Foodservice distributors have developed sophisticated systems to ensure the quality and safety of the products they distribute and to evaluate, and enforce, every aspect of their safety and security systems. The goal is to ensure that procedures currently in place are vigorously enforced, reviewed and improved upon where possible and new ones implemented as necessary.

This guide may assist in planning and implementing protective measures to prevent or minimize the potential for attacks on the food supply. It is not intended to suggest that the measures discussed below are comprehensive, necessary, appropriate or desirable for any specific foodservice distribution operation. Rather, companies should assess, modify and enforce all procedures currently in place, including inbound and outbound transportation and warehousing. They also should scrutinize this document, together with other available resources on this subject (including views of appropriate federal and state agencies) and formulate individualized programs to minimize threats of the type discussed to the greatest extent possible.

## II. THREATS

According to a recently published guide by the United States Air Force on Food Safety and Security, four primary classes of agent pose a potential threat to food products. Those agents are:

- 1.** Biological agents that are delivered in the form of liquids, aerosols or solids (e.g., Salmonella and E. coli). Biological attacks would generally be silent at the time of occurrence and become apparent only later, through the accumulation of severe illnesses in the population.
- 2.** Chemical agents that can be delivered as airborne droplets, liquids, aerosols or solids. They are generally classified as classical chemical warfare agents (nerve, blister, blood and choking agents) and toxic industrial chemicals (e.g., pesticide, rodenticides and heavy metals).

Characteristics of food contaminated by chemical warfare agents include:

AGENT	TASTE	SMELL	COLOR
Mustard	Affected	Garlic	Meat discolored
N-Mustard	Affected	Fishy	No discoloration
Arsenicals	Acidic	Unpleasant	Meat and vegetables discolored
Nerve	Not affected	None	No color change
Cyanide	Bitter almond	Bitter almond	No color change
White phosphorous	Acidic	Garlic	Glow in the dark

3. Radiological agents are radioactive elements that can be delivered in liquid or solid form.
4. Physical agents are materials that could cause adverse health effects if eaten (e.g., bone slivers, glass fragments and metal filings).

When addressing security procedures, it is desirable to consider key safeguards to protect against each of these types of threats.

When assessing your current security capabilities and processes, it is important to keep in mind four basic methods in which a threat could be carried out against a foodservice distribution facility. The four basic tactics that an aggressor could use in an effort to tamper with the food supply are:

1. Exterior attacks that damage facility assets and introduce an agent from outside the facility and/or asset.
2. Forced entry by using tools to enter a facility through an existing passage or to create a new opening in the facility in order to gain access to the facility's contents.
3. Covert entry by using false credentials or other means of deception or stealth in order to gain access to the facility's contents.
4. Insider compromise by using someone with legitimate facility access to tamper with food products.

It is important to develop an action plan that effectively addresses each of these potential contamination methods while remembering that both external and internal threats are possible.

### **III. OPERATIONAL RISK ASSESSMENT AND PROCEDURES**

Ensuring the safety of the food supply has always been a high priority for the foodservice distribution industry. In light of recent events, companies are acutely aware that they have entered a new era of security and, as a result, are examining current procedures and processes. Companies are well aware of the critical control points (by virtue of the industry's experience in dealing with food safety on a daily basis) and are encouraged to review current security precautions to make sure that safeguards are as robust as they can be.

There is little point in speculating on the various means that might be used to carry out any threat to contaminate or tamper with the food supply. However, it is important to remember that human intervention is required before contamination can take place. Therefore, precautionary measures should focus on eliminating any opportunities for contamination or product tampering.

Following are basic measures that foodservice distributors may choose to implement to increase security within their organization. These procedures may assist in preventing or minimizing any attempts to introduce contaminants into the food supply. It must be noted that distributors currently have plans and procedures in place to effectively safeguard their food supplies. The procedures listed below are intended to assist distribution executives by providing a range of options to consider as they work to monitor and improve current systems and procedures in an effort to deter future threats. In order to make the information more actionable, the following

section has been divided into the following risk assessment sections: general, people, sourcing, facilities, systems and transportation.

### **General**

- Implement your version of Hazard Analysis and Critical Control Points (HACCP). By regarding human intervention at any point in the food supply chain as a serious potential hazard, it should be possible to review existing plans and extend them to cover any new potential threats to food security. A rigorous enforcement of your HACCP plan will give your customers confidence that your products and working environment are secure.
- Identify specific procedures for investigating any food security situation that might be identified.
- Assign responsibility for all aspects of security to specific individuals.
- Test alarm and security systems periodically to ensure they are functioning properly.
- Develop a plan to identify and contain mislabeled products.
- Check the safety and security of all utilities, especially water.
- Make sure customers and freight forwarders understand they are responsible for their own on-site product safety.
- Request that all mail from your suppliers and customers carry the sender's company name or logo.
- Advise your mailroom not to open any suspicious mail. Take any unopened, suspicious letters or packages outside into the fresh air while you conduct further investigations and notify the proper authorities.
- Ask all of your staff to refrain from having personal mail sent to your offices.
- Develop clearly documented, well-rehearsed product recall plans with crisis management teams that can quickly assess the scope of any potential problems.
- Create, maintain and distribute lists of the names and phone numbers of all regulatory and law enforcement agencies.
- Immediately investigate and document all reports of unusual activity.
- Develop procedures for handling damaged and/or returned products.
- Monitor and maintain awareness of all warnings and alerts issued by government agencies that deal with crime, threats, safety, health and security.

### **People**

- Review hiring procedures, and verify references of all potential employees.
- To the extent consistent with federal and state law, conduct random drug and criminal background checks on all employees.
- Mandate that each department keep a roster of employees working on any given day. Know who is and who should be on the premises and where they should be located.

**OPERATION THREAT & RISK ASSESSMENT**

- Provide staff with photo identification cards and/or key-swipe cards.
- Provide visitors with an ID badge. Never allow visitors to be unescorted in your facilities.
- Pay special attention to the actions of lumpers. Limit lumper mobility within the facility.
- Review outside driver guidelines and limit outside driver mobility within your facilities.
- Check all incoming engineers and contractor staff, and do not allow any unnecessary tools, etc., to be taken into any distribution facility. Limit contractors' access to those areas of the plant relevant to their work.
- Maintain a vendor "in and out" log for all non-company personnel.
- Ask suppliers and contractors to assign the same people to visit your operations each time, if possible.
- Introduce color-coded hats or garments to help supervisors quickly recognize if someone is out of place.
- Limit the number of personal belongings (purses, gym bags, thermoses, drink containers, etc.) that may be brought to the facility.
- Have employees store clothes and other personal belongings in designated areas separate from food storage and/or preparation areas.
- Ensure that no staff can carry anything onto the distribution floor from the outside, especially from locker rooms.
- Train and discuss with all staff the implications of security/crisis management. Ensure that everyone understands his or her role in the event of a security breach.
- Create an incident response team at every facility.
- Train your employees to recognize and report suspicious activity. Reward and hold all staff accountable for being alert to and reporting signs of product tampering.
- Place all new employees on the day shift with increased oversight during probation.
- Train all employees about food safety and security.
- Develop procedures to ensure that proprietary food security details are kept confidential.
- Supervise maintenance and sanitation staff.

**Sourcing**

- Use known suppliers and contractors, and ask suppliers to implement the same precautions you are taking. Ensure all your suppliers have heightened security and quality assurance procedures in place.
- Review the sourcing of any raw materials, if applicable, and reassure yourself of their integrity and security.
- Require that all suppliers and shippers take whatever actions are necessary to ensure product safety, including the safe delivery of product to the distributor's property and the safe performance of all delivery personnel.
- Obtain food products only from sources that are licensed and regulated by government agencies.

**OPERATION THREAT & RISK ASSESSMENT**

- Include food safety and security measures in purchase contracts.
- Mandate that your suppliers place a unique product number and bar code on all shipping containers. This will increase traceability in the event of a product recall or withdrawal.

**Facilities**

- Account for all keys to each facility.
- Increase all visible levels of security in your distribution centers.
- Develop programs to prevent security breaches with respect to control panels, air circulation lines, electrical boxes, gas and pressure valves, etc.
- Check all perimeter lights, and illuminate exteriors of buildings where food is stored.
- Restrict roof access to authorized personnel. Remove all exterior ladders leading to the roof. Move all waste containers, trees and other climbing tools away from buildings. Secure all roof hatches with an interior padlock, with keys maintained under management control.
- Minimize the number of entrances to controlled areas.
- Consistent with OSHA requirements on means of egress, provide locks for entry doors, windows and roof openings. Make certain all are locked when not in use.
- Minimize the number of gates in perimeter fencing and keep them locked at all times. Remove all clutter from fences and gates.
- Consider adding video cameras and undercover patrols to the interior and exterior areas of your distribution centers.
- Ensure that only authorized persons enter your facilities, and limit access to high-risk/vulnerable environments. If applicable, restrict access to food preparation areas to authorized personnel only.
- Increase security on inbound docks, and ensure all products arriving at your distribution centers are safe, have been inspected by a qualified inspector and have not been tampered with.
- Hold labels in a secure area to prevent theft and misuse.
- Inspect all of your outgoing shipments to ensure they have not been tampered with.
- Eliminate places within facilities where a contaminating agent could be temporarily hidden before being delivered to its target.
- Maintain timely and accurate inventory of hazardous chemicals.
- Perform random, unannounced inspections of all facilities.

**Systems**

- Immediately delete all facility and computer access capabilities when access authority is rescinded for any employee or after an employee has been terminated.
- Ensure you have adequate computer security, including hardware, software, passwords, paper records and e-mails from unknown sources.

**Transportation**

- Perform random inspections of all vehicles.
- Require that all inbound shipments arrived locked and sealed. Verify shipping seals with shipping papers.
- Secure/lock trucks at all times when delivering products to customers. Use serial numbered seals on vehicles shipping food products. Note these numbers on shipping papers. Verify shipping seals with shipping papers.
- Require transportation companies to conduct criminal background checks on all drivers.
- Implement lock program on storage and drop trailers.
- Develop and implement security procedures for drivers to adopt when stopping for meals, gas, breakdowns, etc.

None of these measures should be considered a one-time action. Most security experts recommend that foodservice distribution companies continuously monitor the effectiveness of implemented control procedures to ensure they are effective and remain in place.

To maximize effectiveness when implementing risk controls, foodservice distributors should consider adopting the following guiding principles when creating and enforcing a risk management plan:

1. Effectively describe the benefits of implementation to employees.
2. Establish clear lines of accountability and responsibility for plan implementation.
3. Obtain senior management commitment and approval.
4. Involve personnel affected by the risk control plan in its development and implementation.
5. Develop comprehensive supporting tools and documents (such as standard operating procedures).
6. Identify reasonable timelines for implementation.
7. Designate a contact and control person(s).

**IV. RESPONSE ACTIONS**

In the event of potential food contamination, evaluate initially the degree to which the threat is real and of significant concern. If you suspect that food might be contaminated, secure it, report it to the proper authorities and hold it until the necessary regulatory authorities determine its condition. If you suspect contamination, the following steps should be taken:

1. Have your designated and trained control person handle all actions.
2. Notify the appropriate regulatory agency and the FBI immediately.
3. Secure the crime scene. Don't allow anyone access to the area.
4. Immediately identify all witnesses. Determine who has had access to the area, and identify people who have handled the product in question or were in the immediate or surrounding areas.
5. Determine who might have been affected by the contamination.

**OPERATION THREAT & RISK ASSESSMENT**

6. Secure all written material associated with the incident.
7. Secure any material that may be used for chemical analysis.
8. After investigation by the regulatory agencies, decontaminate any surfaces and tools that might have come in contact with the food in question.
9. Shut down the facility until all areas have been sanitized and the appropriate regulatory agency determines what type of contaminant, if any, is present.