United States Department of Agriculture

Food Safety and Inspection Service

October 2009

Food Defense Guidelines for Slaughter and Processing Establishments

This publication supersedes
FSIS Security Guidelines for Food Processors

These updated *FSIS Food Defense Guidelines for Slaughter and Processing Establishments* are designed to assist Federal- and State-inspected facilities in developing preventive food defense measures. Operators are encouraged to review their current procedures and controls to address the potential for intentional and unintentional, contamination and make appropriate improvements.

What Is Food Defense?

Food safety addresses the unintentional contamination of food products during processing or storage by microbial, chemical, or physical hazards (foreign objects). This accidental contamination of food products can be reasonably anticipated based on the type of processing. Food defense, on the other hand, focuses on protecting the food supply from intentional and unanticipated contamination with various chemical and biological agents or other harmful substances by people who want to do harm. These agents could include materials that do not occur naturally or are not part of routine food product testing. An attacker's goal might be to harm or kill people or to disrupt our economy. Intentional acts are hard to predict.

Why New Guidelines?

This list of recommendations replaces the agency's first set of guidelines on food defense issued in 2002, *FSIS Security Guidelines for Food Processors*. These are based on information learned from vulnerability assessments FSIS has conducted. The guidelines are intended to meet the particular needs of FSIS-regulated facilities and to be readily adaptable for each operation. **FSIS recognizes that not all of the guidance in this document will be appropriate or practical for every facility.** Operators should review each section of the guidelines that relates to a component of their operations and assess which preventive measures are suitable. While these guidelines are voluntary, and operators could choose to adopt measures other than the ones suggested, it is vital that all food businesses take steps to ensure the security of their facility and food products.

Why It Matters to You

An attack on the food supply can be carried out by an organized extremist group, but it also can be carried out by a disgruntled employee or result from an incident in your community (e.g., local citizen protest). While your individual facility might not be directly at risk, there is a high likelihood that an attack occurring even at one establishment will likely impact that entire industry, including international trade. Put simply, it is good

business practice to address food defense—***it protects your business, your employees and your product***.

How a Food Defense Plan Helps

A key component to protecting the food supply is to develop a food defense plan. This plan provides an opportunity to identify areas where security measures could be enhanced. Once implemented, the plan will help focus employee training and response and recovery actions. Key areas include:

- inside and outside security,
- slaughter and processing security,
- storage security,
- shipping and receiving security,
- water and ice security, and
- mail-handling security.

There are many potential benefits of having an effective food defense plan in place such as:

- Protects public health and assets;
- Possibly reduces insurance premiums and freight rates;
- Increases public and customer confidence, including trading partners;
- Provides value-added component to product;
- Deters theft and tampering;
- Creates production and distribution efficiencies; and
- Maintains greater control over product through supply chain.

The overall plan should strengthen these areas to protect your facility and products. FSIS has developed guidance on developing a food defense plan that can be found on the Internet at: **http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Guidance_Materials/index.asp.**

Whether you use FSIS' food defense plan guidance or some other source, the recommendations in this booklet still will provide you with useful information on what elements to consider and address.

For questions or clarification about these guidelines, contact the FSIS Office of Data Analysis and Food Protection at 1-202-720-5643.

Find these guidelines and other helpful food defense information at:

FSIS Food Defense Guidelines for Slaughter and Processing Establishments*
http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Guidance_Materials/index.asp

FSIS Safety and Security Guidelines for the Transportation and Distribution of Meat, Poultry, and Egg Products*
http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Guidance_Materials/index.asp

FSIS Developing a Food Defense Plan for Meat and Poultry Slaughter and Processing Plants*
http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Guidance_Materials/index.asp

FSIS Guide to Developing a Food Defense Plan for Warehouses and Distribution Centers*
http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/Guidance_Materials/index.asp

Guidelines for the Disposal of Intentionally Adulterated Food Products and the Decontamination of Food Processing Facilities
http://www.fsis.usda.gov/PDF/Disposal_Decontamination_Guidelines.pdf

FSIS Podcasts on Food Defense (audio and video)
http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/../../News_&_Events/Food_Safety_Inspection_Podcasts/index.asp

World Health Organization (WHO)—Terrorist Threats to Food—Guidelines for Establishing and Strengthening Prevention and Response Systems (ISBN 92 4 154584 4)
http://www.who.int/foodsafety/publications/general/terrorism/en/

U.S. Food and Drug Administration (FDA)—Food Defense & Terrorism
http://www.cfsan.fda.gov/~dms/defprog.html

U.S. Food and Drug Administration (FDA)—Food Security Preventive Measures Guidance for Processors, Importers, Transporters, Food Service, and Retailers
http://www.cfsan.fda.gov/~dms/defguids.html

USDA, Food and Nutrition Service (FNS) A Biosecurity Checklist for Food Service Programs, Developing a Biosecurity Management Plan
http://healthymeals.nal.usda.gov/hsmrs/biosecurity.pdf

**Some publications are available in multiple languages.*

Food Defense Plan Management

- ❏ Designate a person or team to develop, implement, manage, and update your Food Defense Plan.
- ❏ Train appropriate personnel in food defense.
- ❏ Conduct regular food defense drills.
- ❏ Keep details of food defense procedures secure.
- ❏ Include emergency contact information for local, State, and Federal Government homeland security authorities and public health officials in the food defense plan. **(Find helpful information on State contacts at: http://www.whitehouse.gov/homeland/contactmap.html.)**
  - ❍ Review and update this contact information regularly.
  - ❍ Designate plant personnel who will initiate contact with these authorities.
- ❏ Include procedures for responding to threats of product contamination in your plan.
- ❏ Include procedures for responding to actual incidents of product contamination in your plan. **(Find helpful information at: http://www.state.tn.us/agriculture/security/fsig.html.)**
- ❏ Have procedures that will ensure that adulterated or potentially harmful products are not distributed in commerce.
- ❏ Have procedures in place for safe handling and disposal of contaminated products in accordance with your Federal or State environmental authorities.
- ❏ Encourage employees to report signs of possible product contamination, unknown or suspicious persons in the facility, or breaks in the food defense system.
- ❏ Include evacuation procedures in your plan. **(Find helpful information at: http://www.osha.gov/dep/evacmatrix/index.html.)**
- ❏ Have procedures in place that restrict access to your facility to only authorized personnel during an emergency.
- ❏ Have a documented recall plan in place that ensures the segregation and proper disposition of recalled products and update the plan regularly.

€

Not all recommendations will be applicable to all facilities.

Outside Security

- ❑ Secure the facility grounds to prevent entry by unauthorized persons (e.g., locked fence, gate, or entry/exit door).
- ❑ Post "No Trespassing" signs at the facility's boundaries.
- ❑ Ensure that there is enough lighting outside the building to properly monitor the plant premises at night and in the early morning.
- ❑ Have self-locking doors and/or alarms in place on all emergency exits.
- ❑ Ensure the following are secured with locks, seals, or sensors when unattended (after hours/weekends) to prevent unauthorized entry:
  - ❍ outside doors and gates,
  - ❍ windows,
  - ❍ roof openings,
  - ❍ vent openings,
  - ❍ trailer (truck) bodies,
  - ❍ tanker truck hatches,
  - ❍ railcars, and
  - ❍ bulk storage tanks/silos.
- ❑ Use controlled-access procedures for people and/or vehicles entering the plant and/or parking in your lot, such as:
  - ❍ using controlled or guarded entrance,
  - ❍ identifying employee vehicles with placards, decals, or some other form of visual identification, and
  - ❍ identifying visitor/guest vehicles using placards, decals, or some other form of visual identification.

Not all recommendations will be applicable to all facilities.

General Inside Security

- ❑ Install an emergency lighting system in the facility.
- ❑ If using security cameras in your facility, monitor them regularly.
- ❑ Use an emergency alert system and test it regularly.
  - ❍ Clearly mark locations of controls for emergency alert systems.
- ❑ Clearly mark all restricted areas (i.e., areas where only authorized employees have access).
- ❑ Restrict visitors, guests, and other non-employees (e.g., contractors, sales people, and truck drivers) to non-product areas unless accompanied by an authorized employee.
- ❑ Have available up-to-date copies of facility layout/blueprints for local law enforcement, including the fire department.
  - ❍ Require county records office to notify you when a copy of your blueprints are requested.

Not all recommendations will be applicable to all facilities.

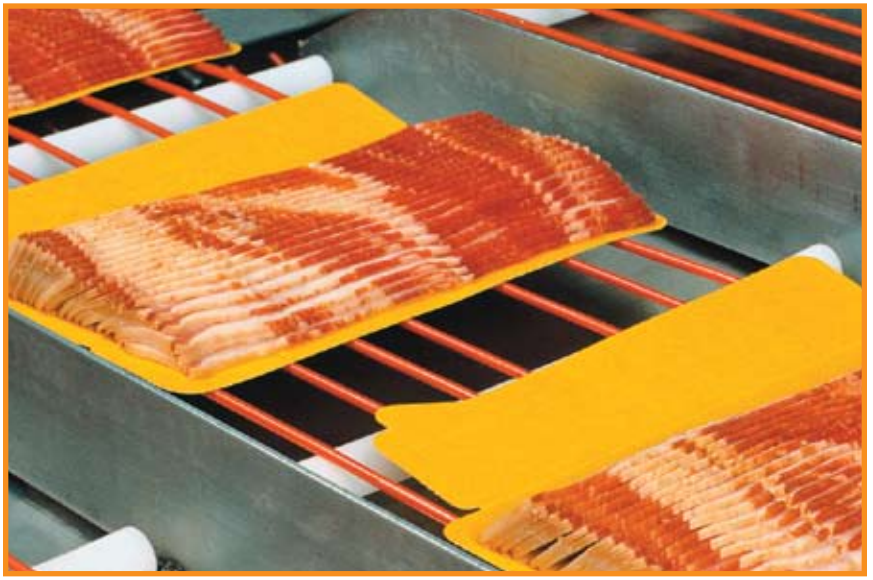
- ❏ Have procedures in place and periodically check maintenance closets, toilets, personal lockers, and storage areas for suspicious packages.
- ❏ Regularly take inventory of keys to secured/sensitive areas of the facility.
- ❏ Ensure that ventilation systems are constructed in a manner that provides for immediate isolation of contaminated areas or rooms, if possible.
- ❏ Limit access to the controls (e.g., by locked door/gate or to designated employees) for the following systems in the facility:
  - ❍ heating, ventilation, and air conditioning,
  - ❍ propane gas,
  - ❍ water,
  - ❍ electricity,
  - ❍ disinfection systems, and
  - ❍ clean-in place systems or other centralized chemical systems.
- ❏ Limit access (e.g., by locked door, pass card, etc.) to the in-plant laboratory facility to authorized employees only.
- ❏ Have procedures in place to control receipt of samples from other establishments.
- ❏ Have a procedure in place to receive and securely store laboratory reagents.
- ❏ Have a procedure in place to control and dispose of reagents.
- ❏ Password-protect access to the facility's computer systems. **(Find helpful information at: http://www.umich.edu/~policies/pw-security.html.)**
- ❏ Ensure that firewalls are built into the computer network.
- ❏ Use an up-to-date computer virus detection system.

Not all recommendations will be applicable to all facilities.

Slaughter and Processing Security

- ❑ Limit access to product production/slaughter and holding-pen areas to facility employees and FSIS inspection personnel only.
- ❑ Monitor production lines that handle and transfer products, water, oil, or other ingredients to ensure integrity.
- ❑ Examine packaging of ingredients before use for evidence of tampering.
- ❑ Maintain records to allow easy trace-back of raw materials to suppliers.
- ❑ Maintain records to allow easy trace-forward of finished products to vendors.

Not all recommendations will be applicable to all facilities.



Storage Security

- ❑ Monitor raw product storage areas, including cold and dry storage areas, for unauthorized personnel.
- ❑ Ensure controlled access to restricted non-meat ingredient storage areas.
- ❑ Maintain an access log for non-meat ingredient storage areas.
- ❑ Ensure controlled access to finished product storage areas.
- ❑ Ensure controlled access to external storage facilities.
- ❑ Regularly conduct security inspections of storage facilities, including temporary storage vehicles.
- ❑ Maintain records on facility security inspection results.
- ❑ Regularly check inventory of restricted ingredients (i.e., nitrites, etc.) against the actual use of such ingredients.
- ❑ Control product labels and packaging to prevent theft and misuse.
- ❑ Regularly check the inventory of finished products for unexplained additions and withdrawals from existing stock.
- ❑ Limit access to inside and outside storage areas for hazardous materials and chemicals (i.e., pesticides, industrial chemicals, cleaning materials, sanitizers, and disinfectants) to designated employees only.
- ❑ Maintain a current inventory of hazardous materials and chemicals.
  - ❍ Immediately investigate discrepancies in daily inventory of hazardous materials/chemicals.
- ❑ Ensure that storage areas for hazardous materials/chemicals are constructed and safely vented in accordance with local building codes.
- ❑ Have a procedure in place to receive and securely store hazardous chemicals.
- ❑ Have a procedure in place to control disposition of hazardous chemicals.

Not all recommendations will be applicable to all facilities.

Shipping and Receiving Security

- ❏ Keep trailers and tankers on the premises under lock and/or seal when not being loaded or unloaded.
- ❏ Closely monitor loading and unloading of vehicles transporting raw materials, finished products, or other materials used in food processing.
- ❏ Seal outgoing shipments with tamper-evident seals.
  - ❍ Document seal numbers on the shipping documents.
- ❏ Inspect tanker trucks and railcars to detect the presence of any material, solid or liquid, in tanks prior to loading liquid products.
  - ❍ Keep records of the inspections of tanker trucks and railcars.
  - ❍ Maintain chain-of-custody records for tanker trucks and railcars.
- ❏ Control access to loading docks to avoid unverified or unauthorized deliveries.
  - ❍ Require advance notification from suppliers (by phone, e-mail, or fax) for all incoming deliveries.
  - ❍ Immediately investigate suspicious alterations in shipping documents.
  - ❍ Check all deliveries against the roster of scheduled deliveries.
  - ❍ Hold unscheduled deliveries outside facility premises pending verification.
- ❏ Require prior notice if off-hour delivery is accepted, and ensure that an authorized person is present to verify and receive the delivery.
- ❏ Check less-than-truckload (LTL) or partial-load shipments for content and evidence of tampering.
- ❏ Require incoming shipments of raw products, ingredients, and finished products to be sealed with tamper-evident or numbered seals (and documented in the shipping documents). Verify the seals prior to entry.
- ❏ At the receiving dock, check incoming shipments of raw products, ingredients, and finished products for evidence of tampering.
- ❏ Notify the FSIS Public Health Veterinarian immediately if you receive animals with unusual behavior or symptoms.
- ❏ Protect feed and drinking water supplies for live animals from possible intentional contamination.

Not all recommendations will be applicable to all facilities.

- ❏ When selecting transportation companies and suppliers, consider the company's ability to safeguard the security of the product/animals being shipped.
  - ❍ Transportation companies should perform background checks on drivers and other employees who have access to product/animals.
  - ❍ Ingredient suppliers should take steps to strengthen food defense in their facilities and during transport.
- ❏ Examine all returned goods at a separate designated area in the facility for evidence of possible tampering before salvage or use in rework.
  - ❍ Maintain records of returned goods used in rework.
  - ❍ Follow the procedures outlined in **FSIS Directive 9010.1** for return of U.S. exported products. **(Find helpful information at: http://fsis.usda.gov/oppde/rdad/fsisdirectives/9010-1.pdf.)**

Not all recommendations will be applicable to all facilities.

Water and Ice Security

- ❑ Restrict access to water wells (e.g., by locked door/gate or limiting access to designated employees).
- ❑ Restrict access to ice-making equipment and storage facilities.
- ❑ Restrict access to storage tanks for potable water and to water reuse systems.
- ❑ Inspect potable and non-potable water lines for possible tampering (i.e., visual inspection for physical integrity of infrastructure, connection to potable lines, etc.).
- ❑ Make arrangements with local health officials to ensure that they will immediately notify the plant if the potability of the public water supply is compromised.

Mail-Handling Security

- ❑ Conduct mail-handling activity in a separate room or facility that is away from in-plant food production/processing operations.
- ❑ Train mail handlers to recognize and handle suspicious pieces of mail using U.S. Postal Service guidelines. **(Helpful information is provided at http://www.usps.com/news/2001/press/serviceupdates.htm).**

€

Not all recommendations will be applicable to all facilities.

Personnel Security

- ❏ Conduct background checks[1] on all employees and contractors (both permanent and seasonal) who will be working in sensitive operations (e.g., grinding area).
- ❏ Train all facility employees on security procedures as part of their orientation training.[2]
- ❏ Identify employees, visitors, and contractors (including construction workers, cleaning crews, and truck drivers) in some manner (e.g., ID badges, colored garb, etc.), at all times while on the premises.
- ❏ Control access by employees and contractors entering the facility during both working hours and non-working hours (e.g., coded doors, receptionist on duty, swipe cards, etc.).
- ❏ Limit temporary employees and contractors (including construction workers, cleaning crews, and truck drivers) to areas of the plant relevant to their work.
- ❏ Use a system to identify personnel by their specific functions/ assignments/departments (e.g., corresponding colored uniforms or hair covers).
- ❏ Prohibit employees from removing company-provided or protective gear from the premises that could be used to gain unauthorized entry into the facility.
- ❏ Maintain an updated shift roster for each shift (i.e., who is absent, who the replacements are, and when new employees are being integrated into the workforce).
- ❏ Do not allow personal items into the production area.
- ❏ Restrict items that employees and visitors can bring into the facility, and provide a list of prohibited items (e.g., cameras).

Not all recommendations will be applicable to all facilities.

1 DHS's e-verify is a free program and can be accessed at **https://e-verify.uscis.gov/enroll/**.

2 Training information is provided at **http://www.fda.gov/ora/training/orau/FoodSecurity/default.htm** or **http://www.fda.gov/Food/FoodDefense/Training/ucm11400.htm**.

NOTES

NOTES