



USDA Food Defense Program

ISAAP 2F

The AMS ISAAP Food Defense Program is an audit program that applies to food manufacturing and/or processing facilities regardless of industry. It is intended to provide applicants [and their customers] with added confidence that they are carrying out recommended food defense practices.

No USDA or AMS logo or statement is allowed to be used in conjunction with this program.

The AMS ISAAP Committee would like to recognize the AMS Food Defense Sub-committee for their collaborative work in developing the requirements for this program.

U.S. Department of Agriculture
Agricultural Marketing Service
Industry Services Audit and Accreditation Programs
July 12, 2012

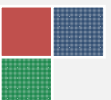




Table of Contents

Section	Title	Page
1	Scope	3
2	References	3
3	Definitions	3
4	AMS Division Responsibilities	4
5	Applicant Responsibilities	4
6	Frequency of Audits	4
7	Program Requirements	4
7.1	Food Defense Management Plan	4
7.2	Personnel Security: Employees, Visitors, Contract Workers, and Others	6
7.3	Security of Perimeter, Buildings, and Docks	8
7.4	Security of Incoming/Outgoing Shipments	9
7.5	Receipt Inspection Security	10
7.6	Production Areas	11
7.7	Warehousing and Storage Security	12
7.8	Control of Hazardous Material	13

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.

Authorized by: Associate Administrator
Document Owner: AMS ISAAP Manager
Authorized Distribution: Public

Current Version Date: July 12, 2012
Original Issue Date: July 12, 2012



1 Scope

1.1 General

This document specifies the requirements for the AMS Food Defense Program.

1.2 Application

All requirements of this document are generic and are intended to be applicable to all applicants, regardless of type, size, and product produced. This document is intended for food manufacturing and/or processing facilities. It may also be applied to warehouses though some requirements do not apply to those types of facilities. It is not intended to be applied at farms.

2 References

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

- 2.1 [FSIS Developing a Food Defense Plan for Meat and Poultry Slaughter and Processing Plants, updated June 2008](#)
- 2.2 [FSIS Guide to Developing a Food Defense Plan for Warehouse and Distribution Centers, dated January 2008](#)
- 2.3 [FSIS Food Defense Guidelines for Slaughter and Processing Establishments, dated October 2007](#)
- 2.4 [FSIS Safety and Security Guidelines for Transportation and Distribution of Meat, Poultry, and Egg Products dated June 2005](#)
- 2.5 [FDA Guidance for Industry Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance dated October 2007](#)

3 Definitions

Additional definitions regarding AMS ISAAP activities are located in ISAAP 1A2 - AMS ISAAP Terminology, Definitions, and Acronyms. The AMS Food Defense Program adopts the definition as outlined FSIS Guide to Developing a Food Defense Plan for Warehouse and Distribution Centers dated January 2008.

3.1 Food defense is putting measures in place that reduce the chances of the food supply becoming intentionally contaminated using a variety of chemicals, biological agents or other harmful substances by people who want to do us harm. These agents could include materials that are not naturally-occurring or substances not routinely tested for in food products. A terrorist's goal might be to kill people, disrupt our economy, or ruin your business. Intentional acts generally occur infrequently, can be difficult to detect, and are hard to predict.

Food defense is not the same as food safety.

3.2 Food safety addresses the accidental contamination of food products during storage and transportation and focuses on biological, chemical or physical hazards. The main types of food safety hazards are microbes, chemicals, and foreign objects. Products can become contaminated through negligence and can occur during storage and transportation.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



4 AMS Division Responsibilities

4.1 The AMS Division shall establish the documented requirements in developing an AMS Food Defense Program. The AMS Food Defense Program shall meet all requirements outlined in this document; exclusions are not allowed.

4.2 The AMS Division may not use an alternative name for an AMS Food Defense Program.

4.3 The AMS Division may use the Food Defense in any program, instruction, or information used to describe the program.

4.4 The AMS Division shall not use the terms "HACCP," "food safety management system," or "management system" "quality management system," "quality system," or "ISO based" in any program, instruction, or information used to describe the program.

4.5 The AMS Division shall select an AMS Auditor who meets the AMS Auditor Criteria for the AMS Food Defense Program.

5 Applicant Responsibilities

The applicant shall develop and implement a documented program that addresses all requirements of the AMS Food Defense Program. The documented program shall include

- a. Documents required by the AMS Food Defense Program;
- b. Documents needed by the applicant to ensure the effective planning, operation, and control of its processes; and
- c. Records required by the AMS Food Defense Program.

6 Frequency of Audits

The AMS Division shall conduct the audit in accordance with a specified time frame stated in an AMS Food Defense Program. However, the program audit shall be carried out at least once annually.

7 Program Requirements

An AMS Food Defense Program shall include the following functional areas based on reference documents in Section 2.

7.1 Food Defense Management Plan

7.1.1 FDA Registration

For FDA regulated facilities, the food defense plan clearly indicates the facility is registered with FDA as per the Bioterrorism Act of 2002. The food defense plan provides the establishment number and the date the facility was registered.

7.1.2 Vulnerability Assessment

A vulnerability assessment is used to develop and implement the Food Defense Plan (for example, using guidance from FDA, USDA-FSIS, industry guidelines, etc.).

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.

Authorized by: Associate Administrator
Document Owner: AMS ISAAP Manager
Authorized Distribution: Public

Current Version Date: July 12, 2012
Original Issue Date: July 12, 2012



7.1.3 Internal Review

The Food Defense Plan is reviewed and reassessed periodically (at least annually) by management to assure it remains relevant to the operation.

7.1.4 Food Defense Manager

The establishment identifies a Food Defense Manager or Coordinator for each facility or company with the overall responsibility to:

- a. Review the adequacy, implementation, and effectiveness of the plan;
- b. Control and secure the plan; and
- c. Receive formal training in principles of food defense and guidance.

7.1.5 Food Defense Team Responsibilities, as applicable

If a team concept is used for Food Defense, each member (by position) of the team is identified and assigned specific responsibilities identified in the plan.

7.1.6 Localized Food Defense Responsibilities

Responsibilities for personnel authorized to monitor and control each area are identified in the plan.

7.1.7 Food Defense Plan Security

Access to the food defense plan is restricted so that the security of the facility is not compromised.

7.1.8 Segregation of Adulterated Product

A procedure is in place to ensure the timely identification, segregation, and security of all products involved in the event of deliberate product contamination. The procedure includes notifying local, State, or Federal Officials in the event of deliberate product contamination.

7.1.9 Maintenance of Food Production Documents and Records

Paper and/or electronic records documenting food production are maintained and controlled.

7.1.10 Employee Food Defense Training

Facility employees receive and document training in food defense. The training includes instructions for employees to immediately report suspicious activity (i.e., external/internal threats, product tampering, etc.) to their supervisor or other management personnel.

7.1.11 Designated Room to Handle Mail

A separate mail handling facility or room is located away from in-plant food production/processing operations.

7.1.12 Mail Handler Training

Employees handling mail are trained to recognize and handle suspicious pieces of mail using U.S. Postal Service guidelines. (<http://about.usps.com/securing-the-mail/best-practices.htm>).

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



7.1.13 List of Officials

The plan provides a current list of local, State and Federal Government Homeland Security contacts and public health official. The list is updated quarterly.

7.1.14 Notification of Officials

The plan identifies a specific procedure for the immediate notification of officials (see clause 7.1.13). The plan includes procedures for handling and investigating situations such as internal/external threats, suspicious activity, actual or potential cases of tampering or other malicious, criminal, or terrorist actions.

7.1.15 Tampering During Evacuation

The plan includes an evacuation plan for each facility for emergencies; such as a bomb threat, fire, flood, chemical spill, etc. and includes provisions to prevent product tampering during the evacuation process.

7.1.16 Food Defense Exercises/Drills

Food defense exercises/drills are conducted to verify key provisions of the plan. The results of these exercises/drills are reviewed and changes made when necessary.

7.2 Personnel Security: Employees, Visitors, Contract Workers, and Others

7.2.1 Employee Background

- a. Prior to hiring, background checks [e.g., employee references and/or immigration status (INS Form I-9)] are conducted on all employees who will be working in controlled access areas of the operations.
- b. If background checks are not required for all employees, the plan identifies which employees (seasonal, temporary, permanent, and contract workers) by position are subjected to background checks before hiring.
- c. Official(s) with the responsibility for ensuring employment references are clearly identified. Background checks, if required, are verified and up to date, and stipulate the required frequency (e.g., semi- annual, etc.) of these reviews.

7.2.2 Employee Agency/Contractor Background Checks

If the establishment sources employees through a temporary employment agency or a contractor, and those employees are assigned to work in controlled areas of the operation, the establishment conducts background checks that provide a similar level of assurance as those performed on facility employees.

7.2.3 Employee Facility Access

Identify the procedure/method used (e.g., photo IDs with expiration dates, company badges, etc.) for controlling access into the plant during both working and non-working hours. These procedures are applied upon entrance at the facility.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



7.2.4 Employee Identification

- a. There is a procedure (e.g., color-coded uniforms or coded badges) to make it obvious when employees move to areas of the facility where they do not have work responsibilities.
- b. Each department keeps an ongoing roster of employees and makes it available to all plant supervisors.

7.2.5 Prohibited Personal Items

There is a written procedure describing the personal items that are prohibited inside the facility and within production areas.

7.2.6 Restricted Access to Terminated Employees

Upon the termination of an employee, there is a procedure in place to immediately restrict access to the facility by this individual.

7.2.7 Visitor Access To Facility

The visitor policy and method used to control entry into the facility requires positive identification for all visitors (e.g., picture IDs, sign-in and sign-out at the gate, reception desk, etc.).

7.2.8 Visitor Access Within the Facility

A procedure is in place to control visitor's (contractors, salespeople, truck drivers, etc.) movement to prevent them from accessing controlled and restricted areas such as production, ingredient storage, chemical storage, etc.

7.2.9 Employee and Contractor Access

The establishment has documented procedures to:

- a. Control the access of contract workers (e.g., sanitation crews, pest control, etc.) to prevent intentional contamination of product.
- b. Control of the facility is limited to only those areas of the plant relevant to the designated employees' or contractors' work assignment.
- c. Ensure contract workers that use contaminants (e.g. pesticides) are escorted by an authorized plant representative while performing work in the facility.
- d. Allow only designated employees or contractors in controlled or restricted areas where product is vulnerable to contamination.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



7.3 Security of Perimeter, Buildings, and Docks

7.3.1 Perimeter Security

- a. The plant perimeter is monitored for signs of suspicious activity or unauthorized entry.
- b. Measures (e.g., fencing or other barriers, “No Trespassing” signs, etc.) are in place to prevent or monitor unauthorized access within the boundaries of the facility premises.

7.3.2 Control of Facility Access

- a. Access points into the facility are controlled using a combination of the following: fences, security guards, alarms, locking devices, surveillance cameras, alarmed emergency exits that have self-locking doors that can be opened only from the inside, or other defense hardware.
- b. Exterior lights are located at exterior entry ways to the facility to allow detection of unusual activities.

7.3.3 Internal Facility Security

- a. Facility management identifies potential unauthorized access areas. Programs are in place to monitor and prevent defense breaches of the following: control panels, ducts for air circulation, pipes, electrical lines/boxes, gas or pressure valves, doors, windows, roof openings, vent openings, trailer bodies, railcars, etc.
- b. Access to central controls for airflow, water systems, electricity and gas are restricted.

7.3.4 Security of Exterior Bulk Tanks

Access to outside storage tanks containing hazardous materials, potable water, and bulk storage tanks are controlled (e.g., locks, seals, sensors, or other methods) at all times.

7.3.5 Truck Inspection

- a. Procedures are in place for inspecting trucks entering the facility.
- b. Incoming and outgoing vehicles/trucks (both private and commercial) are inspected for unusual cargo or activity.
- c. Upon request, truck drivers are required to present identification prior to entering the facility/gate.

7.3.6 Truck Deliveries

Deliveries are verified against a roster of scheduled deliveries. Unscheduled deliveries are held outside the plant premises, if possible, pending verification of shipment and cargo.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



7.3.7 Driver Security

There is a waiting room for truck drivers that does not allow their unauthorized access to controlled areas of the facility.

7.3.8 Visitor Parking

Parking areas for visitors are monitored and situated at a safe distance from the main facility. Visitor parking area is segregated from production areas, storage, utilities, fuel tanks, etc. by adequate fencing or other means.

7.3.9 Vehicle Identification

Vehicles of authorized visitors, guests, and employees are clearly identifiable (placards, decals, etc.).

7.4 Security of Incoming/Outgoing Shipments

7.4.1 Review and Maintenance of Delivery Records

Records are reviewed and maintained for all delivery conveyances (e.g., tankers, railcars, ships, etc.) used to transport packaging materials, ingredients, and food products used during production and packaging. Shipping documents with unexplained alterations are thoroughly investigated. There is guidance for this type of incident.

7.4.2 Deliveries During Non-operational Hours

There is a policy for deliveries during non-operational hours to ensure prior notice of such deliveries and to require the presence of an authorized individual to verify and receive the shipment.

7.4.3 Delivery Advanced Notice

There is an advance notification (by phone, e-mail, fax, etc.) required for all incoming/outgoing deliveries, including pertinent details about the shipment and the name of the driver.

7.4.4 Use of Seals

- a. There is a requirement for incoming/outgoing shipments to be sealed with tamper-proof, numbered seals and seal numbers are recorded on the shipping documents/bill of lading.
- b. Seal numbers are verified prior to entering/leaving the facility and are registered/logged for each incoming/outgoing shipment.
- c. Seals are inspected for possible tampering.
- d. Transport vehicles are used to transport finished product and are sealed according to customer specifications.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



7.4.5 Loading Dock Security

Procedures are in place to prevent unverified or unauthorized deliveries and for handling deliveries to this area.

7.4.6 Truck Security During Loading

Standard operating procedures are in place to ensure that open trucks are not left unattended during off-loading and loading, and that the shipments are sealed immediately after loading. There is a documented procedure in place to demonstrate that trailers are inspected prior to loading.

7.4.7 Driver Procedure

There is a documented procedure for drivers to:

- a. Keep trailers secure at all times;
- b. Immediately report suspicious activity and any instances of suspected adulteration or tampering with the shipment;

Drivers are provided a list of telephone numbers of officials to contact during operational and non-operational hours.

7.5 Receipt Inspection Security

7.5.1 Tampering of Packages

Procedures are in place for inspecting packages for evidence of intentional tampering.

Tamper-evident packaging features are used when available for ingredients and supplies.

7.5.2 Receiving Employee Training

Receiving employees are trained to look for obvious signs of tampering and to verify the integrity of incoming shipments and products.

7.5.3 Delivery Reconciliation

All deliveries are checked against orders made. Packaging/packing integrity is inspected at the receiving dock for evidence of tampering.

7.5.4 Delivery Acceptance

“Accept” and “Reject” criteria for all incoming materials are well understood by personnel receiving products, including courier packages of minor ingredients or laboratory materials.

7.5.5 Product Identification

Incoming materials have clear, legible lot codes.

All lot codes for incoming ingredients, processing aids and packaging materials are identified on production records to ensure that products are traceable from receipt through production to finished products.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



7.6 Production Areas

7.6.1 Water and Ice Security

There is a documented procedure with records in place to establish and support restricted access.

a. Water Source

The plan identifies all sources of water used in the facility (both potable and non-potable). Defense measures are established for each source of water.

b. Notification of Water Tampering

If a municipal water supply is used, there is a procedure to immediately notify local municipal/health officials in the event of any abnormalities or if the water supply in the facility is compromised.

c. Water Line Inspection

Records are available to show that water line access points in food processing areas are inspected regularly to prevent tampering.

d. Ice-making Equipment and Storage

In-plant ice-making equipment and ice storage facilities are monitored, and access to this equipment is controlled.

7.6.2 Ingredient Safety

a. Equipment Monitoring

A procedure is in place to monitor the operation of equipment (blenders, choppers, chill tanks, etc.) to prevent product tampering.

b. Maintenance of Restricted Ingredients

The plan includes daily verification of the projected and actual use of restricted ingredients. Restricted ingredients are verified each day by someone other than the employee who logs the ingredients.

c. Ingredient Tampering

The plan includes the integrity of packaging materials of all spices and restricted ingredients (including premixes prepared in the plant) are verified prior to use. Accountability programs, such as “sign-off sheets” for all restricted ingredients are utilized. There is a list of personnel authorized to handle restricted ingredients.

7.6.3 Laboratory Control

a. Controlled Access

Access to in-plant laboratory facilities is controlled.

b. Mercury Thermometers Accountability

Mercury in glass thermometers are accounted for on a daily basis, as applicable.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



- c. Control of Laboratory Materials
Only sample collection laboratory materials are permitted on the manufacturing floor.
- d. Chemical Inventory
An up-to-date inventory of all hazardous laboratory chemicals and solvents is maintained. Access to these materials is restricted.

7.6.4 Batching/Mixing

- a. Restricted Access
Access to product production or holding areas is controlled.

Mixing or batching of product or ingredients is monitored to prevent employee tampering, especially in areas where employees are by themselves without supervision or a coworker present.
- b. Batch Access Points
Points in the batching process are identified where access creates vulnerability. These access points will be monitored.
- c. Restricted Bulk Areas
Areas where large amounts of exposed product is present (e.g. vats, kettles, tanks, chillers, coolers, etc.) are controlled to limit access.
- d. Ingredient/Packaging Traceability
All ingredient components, packaging materials (that come in direct contact with food), etc., used in the production of finished products are recorded or maintained in case of a recall.
- e. Reworked Product
There are specific procedures and records in place that establish how product is to be reworked during processing.
- f. Intentional Contamination
The plan identifies procedures to follow in the event an intentional contamination occurs during production.
- g. Processing Systems
Processing systems, including automatic control systems, are secure.

Individuals with access to control systems are identified.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



7.7 Warehousing and Storage Security

7.7.1 Manager Identified

The persons in charge of warehousing and storage security are clearly identified (by positions).

7.7.2 Controlled Access

A procedure is in place that controls access to stored product minimizes the possibility of product adulteration/tampering.

The plan identifies all storage facilities used to store ingredients, products, and materials.

7.7.3 Storage Area Security

The plan includes security of all areas in which products and ingredients are handled and stored (e.g., off-site warehouses, product chillers, and storage facilities).

7.7.4 Identification of Restricted Areas

Restricted areas inside the plant are clearly marked, secured, and have controlled access.

7.7.5 Reworked Product

Procedures and records are in place for handling damaged and/or returned products. These products are inspected for evidence of possible tampering before salvage or use in rework.

7.7.6 Inventory Reconciliation

An inventory of finished product in the warehouse (including location) is maintained that allows the detection of unexplained additions to or withdrawals from existing stock.

7.7.7 Label Control

Labels are stored in a secure area to prevent theft and misuse. There is a plan in place to identify and contain mislabeled products.

7.8 Control of Hazardous Material

7.8.1 Restricted Access

Procedures and physical barriers (e.g., locks or keyed access by authorized personnel only) are in place to restrict access to hazardous compounds such as cleaning and sanitizing chemicals, pesticides, food additives, etc.

These materials are labeled to appropriately indicate their content.

7.8.2 Reconciliation

A daily inventory and material usage log is maintained for hazardous materials and all discrepancies are investigated immediately.

Material Data Safety Sheets are up to date, readily available, and accessible in case of emergency.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.



7.8.3 Segregation

There is a procedure to ensure that cleaning and sanitizing chemicals, lubricants, paints, pesticides and other non-food chemicals are stored away from food processing areas.

7.8.4 Disposal

Comprehensive disposal procedure is in place, particularly for the control of hazardous materials.

To verify the correct version of this document consult the Master Document folder on the AMS ISAAP AGNIS Web site.

Authorized by: Associate Administrator
Document Owner: AMS ISAAP Manager
Authorized Distribution: Public

Current Version Date: July 12, 2012
Original Issue Date: July 12, 2012