

Privacy Impact Assessment

Automated Import Information System (AIIS)

- Version: 2.2
- Date: July 13,2012
- Prepared for: Food Safety and Inspection Service (FSIS), Office of International Affairs (OIA)





Document Revision and History			
Revision	Date	Author	Comments
2.0	January 2007	Katrin Jones	Reformatted and reorganized
2.1	March 2007	Katrin Jones	Revised for accuracy
2.2	July 13, 2012	Mark Whitaker	Updated to reflect new department template (from August 2010) and add in comments from the AIIS team and Privacy Office team.

Abstract

This document serves as the Privacy Impact Assessment for the Automated Import Information System (AIIS). The purpose of the system is to allow FSIS to track shipments of meat and poultry products once they enter the country. The system is user-friendly for inspection personnel, and allows managers easier access to inspection reports. In addition, the AIIS application stores the reinspection results including labeling compliance, condition of containers, product compliance for defects, other foreign material, and laboratory sample results for microbiological, chemical, and drug residues. Any product that fails reinspection and is subsequently refused entry is also entered into the system.

Overview

The Automated Import Information System (AIIS) is a Major Application. The AIIS application provides FSIS with a means of allocating import reinspection assignments for imported meat and poultry in a consistent manner based upon foreign inspection system performance. AIIS functionality includes reporting, trend analysis, and oversight of the inspection force in establishments that export meat and poultry to the United States. The focus of AIIS is on a foreign country's inspection system as a whole, rather than on individual plants. The system uses a statistically based sampling process (based on the annual volume of shipments from the exporting country) to select import shipments for reinspection. The AIIS system links inspectors at all points-of-entry, allowing information on shipments and violations to be shared immediately. While all imported products are inspected in the country of origin, FSIS reinspects all shipments for proper certification documentation, transportation damage, proper labeling, general condition, and box count. Before being released by FSIS, the AIIS application selects shipments for additional reinspection verification. The additional reinspection tasks could include testing for residues, microbiology, or food chemistry. The information stored in this system includes:

- Country of origin
- Foreign production establishment
- Inspection House (name and number)
- Unique shipping mark
- Foreign health certificate
- Customs entry number
- Type of product (name [or a description] of the food product)
- Species
- Number of units
- Net weight
- Employee Name (First and Last)
- Employee ID

AIIS allows FSIS to track shipments of meat and poultry products once they enter the country. The system is user-friendly for inspection personnel, and allows managers easier

access to inspection reports. In addition, the AIIS application stores the reinspection results, including labeling compliance, condition of containers, product compliance for defects, other foreign material, and laboratory sample results for microbiological, chemical, and drug residues. Information about any product that fails reinspection and is subsequently refused entry is also entered into the system and stored.

AIIS resides on a virtual server platform that is configured with operating system (OS) and the AIIS application software. For system input, the Import Inspector receives a completed FSIS Form 9540-1, Import Inspection Application and Report from the importer/U.S. Customs Broker, along with the foreign health certificate. The inspectors enter the shipment data directly into the AIIS database. The outputs are:

- Imported Meat and Poultry Products Presented for Reinspection and Rejected Report;
- Program Management Reports, including:
 - Number of Lots and Net Weights by Countries
 - Disease Status in Eligible Countries
 - Sampling Schedule
 - Intensified Status
 - Refused Entry
 - Possible “Failures to Present,” and
 - Inspection Results Not Completed
- Reports to Foreign Countries (New Zealand, Australia, Canada);
- Report to Congress; and
- Ad hoc reports upon request.

After the Customs and Border Protection (CBP) and the Animal and Plant Health Inspection Service (APHIS) requirements are met, the shipment must be inspected by FSIS at an approved import inspection facility. An FSIS inspector enters information about the shipment into AIIS. AIIS scans its memory bank (AIIS database tables) to determine if the country, plant, and product are eligible for export to the United States. When the shipment is ready to be reinspected by FSIS, AIIS will generate an inspection assignment, based on the plant and country’s compliance history for that specific product. After completing the inspection, the FSIS inspector enters inspection results into AIIS, helping to establish the level of reinspection for future shipments from the plant and the country.

When a shipment is ready to be reinspected, the importer makes a request to FSIS (by submitting a copy of the FSIS Form 9540-1 prior to the shipments arrival). The receipt of the FSIS 9540-1 by Import inspection personnel usually coincides with the arrival of the container ship (the FSIS 9540-1 is usually provided by the broker via overnight courier). The assignment is generated by AIIS at the time the shipment is presented for reinspection at an approved import facility.

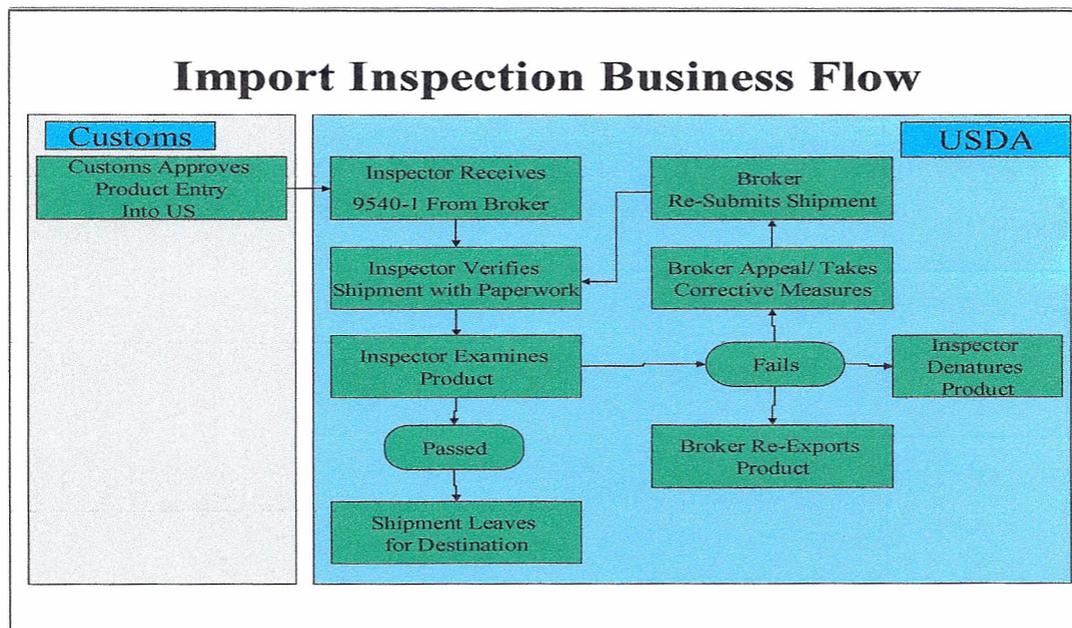
Shipments are declared failure-to-present (FTP) shipments if they are not presented for reinspection by the expected estimated time of arrival (ETA) - 72 hrs for Canadian shipments and 10 days for all other countries – of making entry into the United States. In all cases, the notification is either made at the time that the product makes entry with CBP and APHIS or

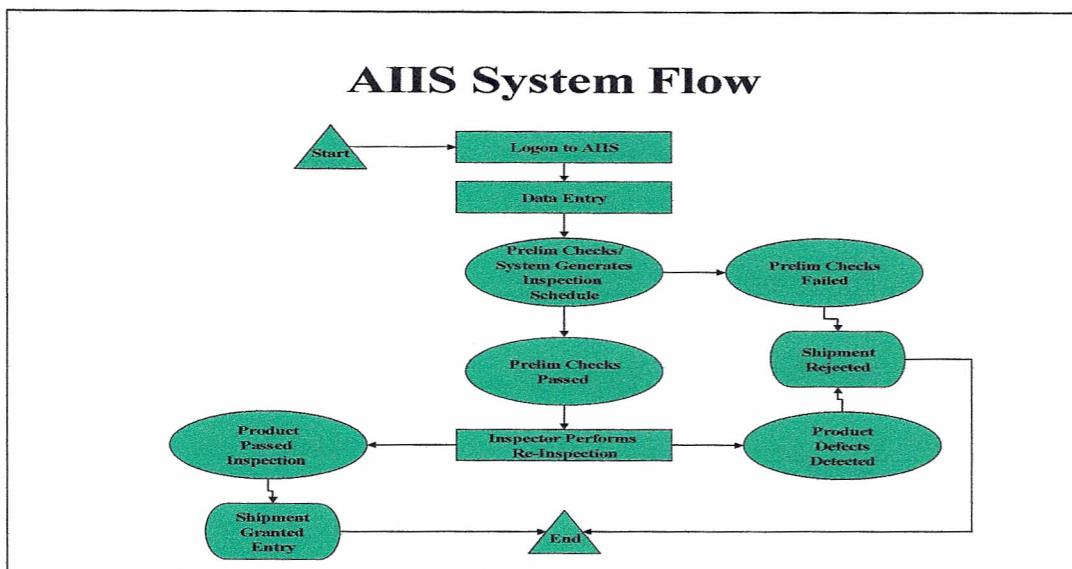
just prior to making entry with CBP and APHIS. The ETA's are noted on each FSIS 9540-1 and are used to help track the shipments and prevent any from bypassing inspection and subsequently be declared an FTP.

FSIS import inspectors first check the documents to assure that the foreign country properly certifies the shipment. Inspection may be delayed or refused if the documents contain irregularities or errors. Inspectors next examine each shipment for general condition and labeling, and then conduct the inspection assignments directed by AIIS.

The AIIS randomly assigns types-of-inspections (TOI's) for each lot presented. At a minimum, every lot is subject to a verification of certifications, labeling, and a general condition. Examples of the TOI's that may be assigned by AIIS include: net weight checks of retail packages; examination of the container's condition; examination for product defects; and laboratory analyses for product composition, microbiological contamination, residues, and species. In conducting these inspections, a certain amount of product is randomly selected and examined by FSIS import inspectors.

Processing Flow





Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

The AIIS system collects, uses, and maintains the general information as noted in the overview. AIIS collects the following personally identifiable information (PII) for federal employees: First Name, Last Name, and Employee Number (all are from the FSIS Active Directory service).

1.2 What are the sources of the information in the system?

For general data, the information sources are the forms provided by the exporting country and establishment, and the inspection results.

All FSIS employee information originates from the FSIS Active Directory, as all FSIS employees must have a user account. When an individual applies for an FSIS Active Directory account, their First and Last Name are provided as part of the request. The Employee Number is derived as part of the process of generating a new FSIS Active Directory user account. When an FSIS user applies for access to the AIIS application, they must already have an FSIS Active Directory account.

1.3 Why is the information being collected, used, disseminated, or maintained?

The general data is collected to help ensure that all imported meat, poultry, and processed egg products are safe, wholesome, and accurately labeled.

The First Name, Last Name, and Employee Number are all used for authenticating the user to the AIIS application. All three items must be present in AIIS for a user to be able to access AIIS.

1.4 How is the information collected?

All FSIS employees must have an FSIS Active Directory user account. When an individual applies for an FSIS Active Directory account, their First and Last Name are provided as part of the request. The Employee Number is derived as part of the process of generating a new FSIS Active Directory user account. When an FSIS user applies for access to the AIIS application, they must already have an FSIS Active Directory account.

1.5 How will the information be checked for accuracy?

The employee's First and Last Name are vetted at the time an employee is hired. The Employee Number from Active Directory is generated at the time the employee's FSIS Active Directory user account is created. If an employee's information is incorrect, they will not be able to access AIIS.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

US Code TITLE 7, CHAPTER 55 - 2204 states that the Secretary of Agriculture may conduct any survey or other information collection, and employ any sampling or other statistical method, that the Secretary determines is appropriate.

The November 18, 2008, amendment to the Executive Order 9397 directs Federal agencies to conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unauthorized use.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The risk is that federal employee First and Last Names are collected and stored in the AIIS system, as is the Employee Number that is generated by the FSIS Active Directory service.

As long as employee name and employee number data are retained, there is the risk that it may be disclosed to unauthorized individuals. To mitigate this risk, the system is maintained in an access-controlled facility and on an access-controlled network. In addition, logical access to the application and data is restricted to authorized personnel.

AIIS System Administrators and general users access the system using unique, authorized accounts. AIIS cannot be accessed without an authorized account and AIIS cannot be accessed by external (non-FSIS) users. There are no anonymous user accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

There are firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. The security controls in the system are reviewed when significant modifications are made to the system, but at least every 3 years. Active Directory and AIIS role-based security is used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory.

When anyone is granted access to the FSIS environment, they are issued a USDA email account and an FSIS user account (managed in Active Directory). To access AIIS, the user must first login to the FSIS network environment by using their Active Directory account to login to their FSIS issued laptop. As a result, their secure network login credentials (from Active Directory) credentials are checked against authorized system user role membership, and access privileges are restricted accordingly. The AIIS user account is used to login to AIIS. When a user accesses AIIS, there are AIIS specific user roles that are used to further restrict a user's access. FSIS system users must pass a Government National Agency Check with Inquiries (NACI) background check prior to having system access. Regular, recurring security training is practiced and conducted through the Office of the Chief Information Officer.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Any contractors who may be authorized to access the system (e.g., software (SW) developers) are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The general data is collected to help ensure that all imported meat, poultry, and processed egg products are safe, wholesome, and accurately labeled.

The First Name, Last Name, and Employee Number are all used for authenticating the user to the AIIS application. All three items must be present in AIIS for a user to be able to access AIIS.

2.2 What types of tools are used to analyze data and what type of data may be produced?

AIIS has a query function that allows records contained within the database to be retrieved based on one or more data elements (e.g. exporting/producing country name, date, inspection house name and number). An analytic component built into the AIIS platform allows the user (the inspector or a supervisor) to review and edit (depending upon the user's role) inspection information records in the system.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

AIIS uses the names of countries and that is exporting food products to the United States. In addition, the names (or a description) of the food products being inspected by an FSIS Inspector are maintained in AIIS. This information is used to track and categorize inspection results by inspection house, country, or by product type (e.g., beef or pork products).

2.4 **Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.**

At the technical level, controls are in place to limit access to AIIS and its data. This helps improve the likelihood of correct handling by limiting access to personnel that know what the application and data are for, and how to use them correctly. As such, AIIS System Administrators and general users access the system using unique, authorized accounts. AIIS cannot be accessed without an authorized account and AIIS cannot be accessed by external (non-FSIS) users. There are no anonymous user accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on

the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

Annual, recurring computer security awareness training is practiced and conducted through the Office of the Chief Information Officer. If users do not take and pass this required training, their access to the FSIS environment (network and applications) as a whole is revoked.

At the policy level, all authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. In addition, there are Agency and Department level policies and directives that, working in tandem with technical controls, help guide and bring about the proper handling of information.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). FSIS keeps accurate accounts of when and to whom it has disclosed personal records. This includes contact information for the person or agency that requested the personal records. These accounts are to be kept for 5 years, or the lifetime of the record, whichever is longer. Unless the records were shared for law enforcement purposes, the accounts of the disclosures should be available to the data subject upon request.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk is that federal employee First Names, Last Names, and Employee Numbers are collected and stored in the AIIS system.

As long as employee name and employee number data is retained, there is the risk that it may be disclosed to unauthorized individuals. To mitigate this risk, the system is

maintained in an access-controlled facility and on an access-controlled network. In addition, logical access to the application and data is restricted to authorized personnel.

See Section 1.7 above for a description of the controls that have been put in place for AIIS and the FSIS environment.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Per the PTA, AIIS receives employee Name alias from the FSIS PBIS application. The alias is the employee's First Name and Last Name, which is used when the employee's Active Directory user account is created; however, AIIS does not provide information to any other internal organizations.

4.2 How is the information transmitted or disclosed?

The AIIS application reads from a PBIS database client that is loaded onto the employee's FSIS workstation.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The PBIS database, and thus the shared information, is loaded onto an FSIS laptop that can only be accessed by an FSIS issued user account. In addition, all FSIS laptops are configured with hard disk encryption to prevent loss of data should an FSIS laptop be lost or stolen.

The PBIS database (local to the workstation) is periodically synchronized with the PBIS database server. To mitigate this risk, the server is maintained in an access-controlled facility and the communications occur over an access-controlled network that is not accessible to the public.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Generally, the AIIS information is not shared with external organizations.

If necessary, information may be disclosed to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Under normal circumstances, AIIS does not share PII outside the department. However, routine use for disclosure to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised. Since the AIIS functionality has been ported to the PHIS application and AIIS will not be needed after September 30th (at the latest), no SORN is being initiated for AIIS at this time.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Should AIIS information need to be shared with NARA, Congress, or Department of Justice, standard FSIS guidelines for providing information to such organizations will be followed.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

As long as employee name and employee number data are transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee information is not shared externally. Such information would only be provided if required by law. Standard FSIS or USDA guidelines for protecting the information would be followed.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to collection of information?

Yes. Employee name information is collected at the point of hiring.

In accordance with Directive 8010.12, if personal information is obtained from an individual, they are provided with a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information. Since the AIIS functionality has been ported to the PHIS application and AIIS will not be needed after September 30th (at the latest), no SORN is being initiated for AIIS at this time.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes.

However, the information is required in order to be hired.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

In accordance with Directive 8010.12, if personal information is obtained from an individual, they are provided with a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

The employee's name is important to the correct authentication of FSIS employees when they attempt to logon to FSIS equipment. If an employee's name is not correct, they will not be able to login to an FSIS laptop or the AIIS application. Furthermore, if their name is not correct, that will affect payroll and other functions. If an employee's information is not being processed correctly, they would work with Human Resources to ensure that the information is correct.

7.2 What are the procedures for correcting inaccurate or erroneous information?

The employee would contact Human Resources and follow the standard HR procedures for addressing incorrect employee information.

7.3 How are individuals notified of the procedures for correcting their information?

New employees are provided with such information at the time they are hired.

7.4 If no formal redress is provided, what alternatives are available to the individual?

N/A- Formal redress is provided.

7.5 **Privacy Impact Analysis**: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Corrections to the data are securely maintained in the same manner as the original data therefore, there is no privacy risk associated with redress available to individuals.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

To gain access to the AIIS system, a user must have (1) an FSIS issue user, (2) a role within the AIIS application, and (3) they must have an FSIS issued workstation.

System Administrators and users of the system will have access. Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

8.2 Will Department contractors have access to the system?

Yes.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Annual, recurring computer security awareness training is practiced and conducted through the Office of the Chief Information Officer. If users do not take and pass this required training, their access to the FSIS environment (network and applications) as a whole is revoked. Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Contractors who may be authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. An access agreement describes prohibited activities (such as browsing) by authorized users is monitored, logged, and audited. All users are required to undergo Department-approved computer security awareness training prior to access and must complete computer security training yearly in order to retain access.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, the Authorization to Operate was granted on August 12, 2011.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database, following and implementing sound federal, state, local, department, and agency policies and procedures are safeguards implemented to mitigate the risks to any information technology.

The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

The primary risks are that the employee's information may be incorrect or that it may be disclosed to unauthorized individuals. These risks are mitigated by the following safeguards.

See Section 1.7 above for a description of the controls that have been put in place for AIIS and the FSIS environment.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

AIIS is an application that has both a client-server component and a web-enabled component. AIIS, through either interface, allows FSIS personnel to track inspection of food products being imported into the United States.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

Both M-10-22 and M-10-23 have been reviewed by the ISSPM team.

10.2 What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

N/A - Third party websites are not being used.

10.3 What personally identifiable information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

N/A - Third party websites are not being used.

10.4 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

N/A - Third party websites are not being used.

10.5 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be maintained and secured?

N/A - Third party websites are not being used.

10.6 Is the PII that becomes available through the agency’s use of 3rd party websites and/or applications purged periodically?

N/A - Third party websites are not being used.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A - Third party websites are not being used.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A - Third party websites are not being used.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A - Third party websites are not being used.

10.10 Does the system use web measurement and customization technology?

N/A

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A - Third party websites are not being used.



Responsible Officials

Jerry Elliott – Director, Import Inspection Division
Office of International Affairs
Food Safety and Inspection Service
United States Department of Agriculture

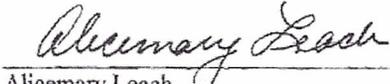
Alicemary Leach – Director, ECIMS
Office of Public Affairs and Consumer Education
Food Safety and Inspection Service
United States Department of Agriculture

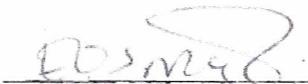
Elamin Osman – Chief Information Security Officer
Office of the Chief Information Officer
Office of the Administrator
Food Safety and Inspection Service
United States Department of Agriculture

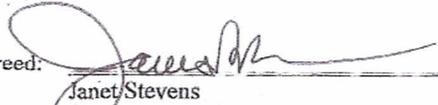
Janet Stevens – Chief Information Officer
Office of the Chief Information Officer
Office of the Administrator
Food Safety and Inspection Service
United States Department of Agriculture

PRIVACY IMPACT ASSESSMENT APPROVALS

Agreed:  7/23/12
Jerry Elliott
Director, Import Inspection Division/System Owner Date

Agreed:  7-19-12
Alicemary Leach
Privacy Officer Date

Agreed:  7/23/12
Elamin Osman
Chief Information Security Officer (CISO) Date

Agreed:  7/30/12
Janet Stevens
Chief Information Officer Date