Privacy Impact Assessment

FSIS Incident Management System (FIMS)

- Version: *1.4*
- Date: 09/21/2012
- Prepared for: Food Safety and Inspection Service

USDA

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	5/2/2008	Eric Penner	
1.1	7/18/2012	Clinton A. Jackson IV	Updated PIA to new format/template. As well as entered updated information after interviewing Lucy Touhey the User Rep.
1.2	08/08/12	James Kurucz	Incorporated comments from Privacy Office
1.3	08/09/12	James Kurucz	Incorporated comments from the ISSB Branch Chief
1.4	09/21/2012	James Kurucz	Incorporated comments from the DCIO

Abstract

This Privacy Impact Assessment is being conducted since FIMS was identified, during the Privacy Threshold Assessment; as using PII. FIMS is a web-based system that allows program managers and users to rapidly identify, respond to, and track the Agency's response to significant incidents. These include suspected tampering of products, threats to facilities, natural disasters, and Class 1 recalls that may affect the nation's commercial supply of meat, poultry and egg products.

Overview

- FIMS is owned and managed by FSIS. The system is housed at the FSIS Enterprise Data Center (EDC) located in Kansas City, MO.
- FIMS is integrated into the FSIS Enterprise Network and is not available to the general public; it is only available to those with access to the FSIS intranet and with an eAuthentication username and password.
- FIMS is not located in a harsh environment that would be detrimental to the hardware or to the system's performance and availability.
- There are numerous roles in FIMS. The key roles include the FIMS Administrator, Emergency Management Committee (EMC) Members, and Technical Support. The functionality that they are responsible for include managing users within the system, creating/updating the information related to IRs, and generating call-down alerts to the FSIS offices.

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?

FIMS collects user's contact information including first and last name, personal cell phone, home phone, FSIS blackberry number and pin, FSIS desk phone and FSIS email addresses.

FIMS also contains information related to specific incidents and may contain the first and last names of establishment employees, first responders, or witnesses to an

incident, and potentially, work or private telephone number contact information for those individuals.

Incident-related information is not retrievable by the individual's name or telephone number.

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

The program area user is the source of the information. They enter it via "my page" which is their own web interface/page to access/update/maintain information.

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

The contact information is collected so that the user can be contacted in the event of an emergency that requires their response or participation.

The incident information is added as it occurs by inspection, enforcement or other FSIS personnel.

1.4 How is the information collected?

The user is the source of the contact information. They enter it via the FIMS "my page," which is their own account/page to access/update/maintain their information.

FSIS personnel are the source of the incident information and any updates to it.

1.5 How will the information be checked for accuracy?

FSIS users are responsible for the accuracy of the information they enter, be it contact or incident information.

The program areas review data for accuracy.

1.6 What specific legal authorities, arrangements, and/or agreements define 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.

44 U.S.C. 3101 states that each USDA mission area, agency, and staff office shall create and maintain proper and adequate documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the

Department of Agriculture (Department) to protect the legal and financial rights of the Government and of persons directly affected by the Department's activities.

Also see: 5 U.S.C. Chapter 552, 44 U.S.C. Chapters 21, 29, 31, and 33 (Records Management), and 18 U.S.C. 2071, 44 U.S.C. 3101 et seq., 44 U.S.C. 3506, Title 7 CFR 2.37, 36 CFR Chapter 12, Subchapter B, 36 CFR Part 1234, eGovernment Act of 2002 (Pub. L. 107-347, 44 U.S.C. Ch. 36), OMB Circular A-130, NARA - Disposition of Federal Records: A Records Management Handbook, NARA General Records Schedules.

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

Access to data is strictly controlled, with access granted through the USDA-approved secure single sign-on application (e-Auth – Level 2 Access) and authorization within FIMS. FIMS is role based to ensure least privileges.

FIMS System Administrators and general users access the system using unique, authorized accounts. FIMS cannot be accessed without an authorized account and it cannot be accessed by external 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 FIMS role-based security are used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system. 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). As noted above, they also have to obtain a USDA e-Authentication account to access FIMS. To access FIMS, the user must first login to the FSIS network environment by using their Active Directory account to login. 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 USDA e-Authentication is used to login to FIMS. When a user accesses FIMS, there are FIMS 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., 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 who are 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.

This information is used to conduct "call downs" that contact users in the event of emergencies, to alert users to activities and incidents that they need to be aware of, and to enable quick participation and response to incidents related to FSIS' public health mission.

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

There are none.

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

FIMS does not use publicly available data.

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.

The controls detailed in Section 1.7 address these risk issues specifically.

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?

Contact information is retained as long as the user has access to the system. Access must be warranted based on user position and status as an employee with FSIS. Incident information is retained for an indefinite time period.

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

No, but FSIS has an overarching data retention policy that has been approved by NARA. Please see FSIS Directive 2620.1 "Records Management Program."

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 length of time data is retained does not affect the type or level of risk. The controls outlined in Section 1.7 provide ongoing privacy protection to the data.

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?

The information is available to all FIMS users to allow for effective management and tracking of significant incidents. This information sharing is the intent of the system. It enables FSIS to respond quickly, effectively, and appropriately to incidents and emergencies.

4.2 How is the information transmitted or disclosed?

Web Interface and by e-mail.

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 risk is that a user might share personal contact data of another user with someone who does not have authority to have that information. FIMS users are routinely provided privacy reminders and take part in annual security awareness training to mitigate that risk. However, the intent of the system is to allow FSIS to respond to food safety and security incidents appropriately and that requires sharing of contact

information. The explicit intent of the system is to enable quick and effective response through the sharing of this information.

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?

Information is not shared with any external organization.

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.

N/A

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

N/A

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

N/A

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?

Users must enter their own information. They are aware of the collection as it is a requirement to access the system.

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

No.

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

N/A

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.

As users enter the data themselves or see the data in the system, there is no lack of awareness, and thus, no risk.

Failure to have this information can lead to greater risks in FSIS being unable to respond to an incident.

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?

Users in specific jobs are identified as having a role that requires FIMS access. The FIMS team must approve them for FIMS access and the user must have an e-Auth level 2 account. Users must then populate their own information in FIMS (or in limited situations, have their administrative assistant populate the information). The FIMS system retains their contact information. Users access "My page" on the system.

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

Users must correct their own information.

In addition, individuals who no longer have access to FIMS but who believe that FIMS might have inaccurate or erroneous PII records pertaining to them should write to the FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 690-3882 Fax (202) 690-3023 - Email: fsis.foia@usda.gov.

The FOIA requestor must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her.

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

When users go on EMC duty they are sent reminders to update information. If there is an emergency and they cannot be contacted, the FIMS team will follow-up to address the situation. Notifications can also be found in the FIMS user manual.

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

See Sections 7.2 and 7.3 of this document.

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

The risk is that a user might share personal contact data of another user with someone who does not have authority to have that information. FIMS users are routinely provided privacy reminders and take part in annual security awareness training to mitigate that risk.

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?

Users must first obtain supervisory requests. Users must have eauth access and must be approved for access to FIMS by the FIMS team in FSIS' Office of Data Integration and Food Protection. This is included in system procedures for FIMS.

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?

Users are required to undergo Computer Security Awareness Training annually as a condition of continued access to the FSIS systems. In addition, FIMS is used by employees who hold positions of responsibility and who are required in their jobs to handle sensitive and confidential information.

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

Yes, ATO granted 3/4/2011.

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

Updates are controlled in that most users can modify only their own information. Only those in administrative assistant or secretarial roles can update their supervisors' information.

FIMS also has activity audit capabilities using three separate reports.

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 controls noted in 1.7, including e-Auth and limited FIMS access, address the general risks. The remaining risk is that a user will share information with someone who is not authorized to have that information. However, the system is used by those in positions of responsibility who are used to handling sensitive and confidential data. This greatly mitigates this risk.

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?

FIMS is a major application.

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"?

N/A. FIMS does not make use of third party applications or websites.

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

N/A

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

N/A

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

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

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

N/A

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

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

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

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 <u>Privacy Impact Analysis</u>: 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

Responsible Officials

Mary Cutshall
System Owner
355 E Street SW Rm 9-140
Washington DC 20472

Elamin Osman
Chief Information Security Officer
1400 Independence Ave SW Rm 4908
Washington DC 20250

Janet Stevens
Chief Information Officer
1400 Independence Ave SW Rm 3165
Washington DC 20250

Alicemary Leach
Privacy Officer
1400 Independence Ave SW Rm 1167
Washington DC 20250

PRIVACY IMPACT ASSESSMENT APPROVALS

Agreed: Mary K Cutshall — 8-9-12
Mary Cutshall — Date
System Owner

Agreed: Elosman — 09/17/12
Elamin Osman — Date
Chief Information Security Officer (CISO)

Agreed: — 9/25/12
Janet Stevens — Date
Chief Information Officer

Agreed: Alicemary Leach — 8-9-12
Alicemary Leach — Date
Privacy Officer