Privacy Impact Assessment

Food Safety and Inspection Service (FSIS) Incident Management System (FIMS)

- Version: 10.0
- Date: July 10, 2023
- Prepared for: Food Safety and Inspection Service (FSIS)

United States Department of Agriculture

Privacy Impact Assessment for the

FSIS Incident Management System (FIMS)

July 10, 2023

Contact Point
Lucy Touhey
Food Safety and Inspection Service (FSIS)
Office of Management (OM)
(202) 309-2607

Reviewing Official
Timothy Poe
Privacy Office
(202) 205-3828

United States Department of Agriculture

Revision History

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.
1.5	06/04/2013	Robin Wagner	Quality Check.
1.6	06/04/2013	James Kurucz	Incorporated Quality Check Comments.
1.7	06/20/2013	James Kurucz	Incorporated System Owner Comments.
1.8	11/13/2013	Robin Wagner	ATO Update.
2.0	09/29/2014	Robin Wagner	Annual Assessment update.
2.1	09/21/2015	Robin Wagner	SO Review for FY 2016 Annual Assessment
2.2	07/31/2016	Robin Wagner	SO Review for FY 2017 ATO
2.3	12/08/2017	Robin Wagner	FIMS FY 18 ATO Review
3.0	07/24/2018	Robin Wagner	FINAL FIMS FY18 ATO
3.1	04/02/2019	Robin Wagner	Review for FY19 A&A

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
4.0	07/18/2019	Robin Wagner	FINAL for FY19 A&A
4.1	04/30/2020	Robin Wagner	Review for FY20 A&A
5.0	06/16/2020	Robin Wagner	FINAL for FY20 A&A
5.1	10/30/2020	Robin Wagner	Review for 2021 ATO
6.0	11/17/2020	Robin Wagner	FINAL for 2021 ATO
6.1	02/17/2021	Robin Wagner	Update to new Privacy Officer and update SO signature.
7.0	05/25/2021	Robin Wagner	2021 ATO Completion
7.1	04/08/2021	Robin Wagner	2022 PIA Template updates from Privacy Office.
7.2	07/01/020022	Robin Wagner	2022 A&A Review
8.0	08/01/2022	Robin Wagner	2022 A&A
8.1	08/10/2022	Robin Wagner	Updates per Privacy Office
8.2	08/23/2022	Robin Wagner	Updates prepping for SORN
8.3	08/27/2022	Robin Wagner	Updates prepping for SORN
8.4	10/14/2022	Robin Wagner	Updates for SORN
8.5	10/21/2022	Robin Wagner	Updates after determining a SORN is not needed.

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
8.6	12/20/2022	Robin Wagner	Updates after deciding HR-GSS will not use the Azure DW server, due to it moving to the Department, and FIMS and HR-GSS sit on the same cloud platform in DISC.
8.7	01/19/2023	Robin Wagner	Updating Sections 4.1 and 4.2 to include table from Tracy Hendrix, USDA Privacy Office, and 6.1 to show FIMS is leveraging 3 SORNs.
8.8	02/01/2023	Robin Wagner	2023 SO Edits for A&A Review
9.0	05/24/2023	Robin Wagner	2023 A&A
10.0	07/10/2023	Robin Wagner	2023 EAT Updates

Abstract

FSIS Incident Management System (FIMS) is a web-based system automating the Incident Response process allowing 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 involve illness.

FIMS offers users ownership, control, and security regarding significant incident and emergency response data allowing efficient and effective support for the nation's food safety and homeland security. FIMS retains the baseline functionality of the previous launch of FIMS. FIMS includes features such as GIS mapping, management of Incident Reports (IRs) and the Emergency Management Committee (EMC), and individual profiles.

FIMS moved from its FSIS Common Enterprise Framework to the Digital Infrastructure Services Center (DISC) Enterprise Cloud Platform (ECP), giving users a single, integrated repository of incident data. In addition, FIMS provides the ability to communicate timely information over a web-based system and run the reports necessary to make strategic decisions.

Overview

- FIMS is owned and managed by FSIS. The system is housed at the Digital Infrastructure Services Center (DISC) 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 e-Authentication (e-Auth) 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 several roles in FIMS having to do with Incident Response. The key roles include the FIMS Administrator, Duty Officer/SEDO, and Executive Manager. Some of these roles may be able to perform the following tasks:
  - Managing users within the system
  - Creating/updating the information related to IRs
  - Generating call-down alerts to the FSIS offices.
- However, not all the above roles can perform these tasks. As an example, only the FIMS Administrator can perform the task of managing users within the system.
- The legal authority for the ATO is the OMB Circular No. A-130, *Management of Federal Information Resources, Appendix 1, Federal Agency Responsibilities for Maintaining Records About Individuals; and Authorization to Operate (ATO).*
- The last FIMS ATO letter is dated 05/25/2021.

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 the user's contact information including first and last name, personal cell phone, home phone, FSIS cell phone, FSIS desk phone, and FSIS e-mail addresses. This information is required input into My Page to be able to work on FIMS, but is not used in incident responses.

FIMS also contains information related to specific incidents and may contain the first and last names of the reporting individual from the establishment where the incident occurred, as well as their position/title, the names of any first responders and/or witnesses to the incident, work or private telephone number, contact information, and/or e-mail addresses for those individuals. Incident-related information also includes Lead District (city and state), location of the incident, originating office, reporting office.

Incident-related information is not retrievable by the individual's name or telephone number. Each incident is identified with a unique incident number within the FIMS Incident Reports (IR) menu. Incidents are retrieved by this number.

FIMS has added the following tables and fields to its DB from Human Resources General Support System (HR-GSS), to be used in the Employee Absenteeism Tracker (EAT):

- roster_dutystation *(table)*
  - state
  - county
  - city
  - code
- roster_officelevel2
  - short_name
  - code
- roster_federalemployee *(table)*
  - empowhr_id
- roster_ohrpemployee *(table)*
  - first_name
  - middle_name

- last_name

- staffing_establishment *(table)*
  - est_num
  - est_name
  - est_city
  - est_state
  - est_zip

With this update, it has been determined that FIMS will leverage the existing HR-GSS SORN, and will therefore not need a SORN of its own.

In this age of remote work, FIMS wants to be able to let the supervisors know where their people are during an event/incident.

Example: In the event of a hurricane coming towards Puerto Rico (PR), the manager will use the EAT to pull the first, middle, and last names, city, state, and zip from HR-GSS for that manager's people working in the PR location. The EAT will attach just their names into the Incident Report (IR) for the hurricane, letting the managers know who their workers are that are working remotely in PR. The managers will export the list from the EAT, and with their names, the managers will be able to contact them.

After the hurricane, the manager will update the EAT for all the ones they can get in touch with, as well as those that are injured, and those they could not reach. The individual EATs will then be rolled up into a Summary Report containing counts of impact that will go up the chain of command. The managers will continue using their exported copy, until all employees are accounted for. And, throughout this event, update the EAT, as the status of these employees is updated, until the end of the event. The exported EAT, if printed, will be shredded after the event.

This information will not be searchable, and the EAT will only be used as a management tool for managers for these types of events/incidents.

The data originating from the above HR-GSS tables/fields will be pulled from within the PostGresSQL database (DB) server maintained in Digital Infrastructure Services Center (DISC) Platform as a Service (PaaS) tables/fields. FIMS will run queries, through an Application Program Interface (API), against the larger HR-GSS dataset. FIMS will then receive the data originating from those HR-GSS tables/fields as input. FIMS will store that data in its PostGresSQL DB server maintained in DISC PaaS. FIMS will then transform that data into an EAT Roll-Up Report that will stay within the USDA.

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

The source of the information within the first paragraph in Section 1.1 above, from the FIMS user. As a mandatory requirement of working on FIMS, the user must input their own information into the My Page portion of the application.

The source of the information within the second and third paragraphs in Section 1.1 above, are the person reporting the incident at the establishment. Once the incident is reported to the FIMS user, the user enters the IR related information via IR menu in FIMS, which is their own web interface/page to create (draft) IR reports. The FIMS user creates, accesses previous reports, submits, views, resubmits, rejects, edits, and approves reports with incident related information.

The source of the data in the fourth paragraph, as stated there, is coming from HR-GSS.

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

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

The incident information is added as it occurs by inspection, enforcement, or other FSIS personnel. This information can also be found in the IR, at times.

The HR-GSS data will be used in the EATs within the FIMS application, and from there, there will be an EAT Roll-Up, which is a report containing only summary numbers, and will not contain any of the data from the tables/fields from HR-GSS. These EAT Roll-Up reports are downloaded by Duty Officers. They will create a Situation Report that includes the numerical summary data to relay to the USDA Office of Homeland Security, Management Council, and the Undersecretary Office. These EAT Roll-Up Summary Reports will stay within the USDA.

1.4 How is the information collected?

The information shown within the first paragraph in Section 1.1 above, is collected by the FIMS user. As a mandatory requirement of working on FIMS, the user must input their own information into the My Page portion of the application.

The incident is reported to FIMS by the reporting individual at the establishment of the incident.

The FIMS user creates the IR within the IR menu of FIMS, using the incident-related information collected from the establishment's reporting individual.

The FIMS API will pull the data from the HR-GSS DB, into the FIMS DB in the DISC PaaS cloud.

1.5 How will the information be checked for accuracy?

FSIS users are responsible for the accuracy of the information they enter on My Page, as well as incident information.

FSIS office is the highest level in the FSIS organization. Administrators maintain offices in FIMS to ensure the FIMS system is accurate and up to date with office changes.

FIMS will rely on HR-GSS to ensure data accuracy, as these fields are their responsibility.

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

The authorities for USDA to collect, maintain, use and disseminate information through this system are: 5 U.S.C.301 (government organization and employees); Title 5 USC 552a (Records Maintained on Individuals (Privacy Act)); Title 41 CFR 201-6.1 (Federal Information Resources Management Regulation); 44 U.S.C.3101 (Records Management); OMB Circular No. A-108 (Responsibilities for the Maintenance of Records About Individuals by Federal Agencies); OMB Circular No. A-130 (Management of Federal Information Resources, Appendix 1, Federal Agency Responsibilities for Maintaining Records About Individuals); and Authorization to Operate (ATO), dated 22-07-14.

In addition, USDA is generally authorized to collect information to support its mission under: Title 7, Chapter 55-2205 (7 U.S.C 2204) (which authorizes the Secretary of Agriculture to collect information and employ any sampling or other statistical method deemed appropriate); 21 U.S.C. 679c(a)(1)-(3) (which expressly authorizes the Secretary to give high priority to enhancing the ability of FSIS to conduct its mission); the Federal Meat Inspection Act (FMIA) (21 U.S.C. 601, et seq.), the Poultry Product Inspection Act (PPIA) (21 U.S.C., et seq.), the Egg Products Inspection Act (EPIA) (21 U.S.C. 1031, et seq.), and the Humane Methods of Livestock Slaughter Act of 1978 (7 U.S.C. 1901-1906).

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 (eAuth – 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 complete set of security controls are tested every three years or when significant modifications are made to the system. Additionally, the USDA has established continuous monitoring, and 1/3 of the controls are now tested as part of the Annual Assessment on the two off years, and the last 1/3 are tested in the third ATO year.

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 requesting access to the FSIS environment, they are issued a USDA e-mail account and an FSIS user account (managed in Active Directory), before being provided access to FIMS. As noted above, they also will be required to obtain a USDA eAuth Level 2 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 are checked against authorized system user role membership, and access privileges are restricted accordingly.

The USDA e-Auth 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 experts in such matters.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

User information on My Page is used for access to the FIMS application, and is used for the duty roster and notifications.

An incident report (IR) is the main artifact of FIMS. IRs are used to track incidents that occur at offices and regulated establishments as well as warehouses that may negatively affect FSIS-regulated products or personnel.

FIMS organizations use Form 5500-8, which is a USDA form, to document the impact of incidents on establishments, warehouses, and import establishments. This document does not track individual FIMS users using PII. FIMS uses an Incident Number to document and keep track of all incidents.

Users can create, edit, and remove 5500-8 forms, as well as view the history of changes made to an IR audit log for each IR. Users can also create and remove 5500-8 roll-ups, as well as view their history. A 5500-8 roll-up consolidates information from all the 5500-8 forms by the office. There are different types of 5500-8 forms: Establishment, Warehouse, I-House, and Office.

This information is used to conduct "call downs" that contact users if emergencies occur, 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.

Users can create, edit, and remove absenteeism trackers, as well as view their history. Users can also create and remove absenteeism tracker roll-ups, as well as view their history. An absenteeism tracker roll-up consolidates employee absenteeism trackers by office and state.

The EMC alert and activation are two ways for users to escalate problems associated with specific IRs. EMC alerts are less critical but indicate an issue. EMC activations are initiated for meetings.

Use of the data from the HR-GSS DB will only be used in reports, periodically, as needed, as listed in the example above in Section 1.1.

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

There are no tools used to analyze the IR data. Data is produced through IR generation. EATs are produced through EAT generation, and does not include PII data.

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.

Access to data is strictly controlled, with access granted through the USDA-approved secure single sign-on application (eAuth – 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 complete set of security controls are tested every three years or when significant modifications are made to the system. Additionally, the USDA has established continuous monitoring, and 1/3 of the controls are now tested as part of the Annual Assessment on the two off years, and the last 1/3 are tested in the third ATO year.

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 requesting access to the FSIS environment, they are issued a USDA e-mail account and an FSIS user account (managed in Active Directory), before being provided access to FIMS. As noted above, they also have to obtain a USDA eAuth Level 2 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 are checked against authorized system user role membership, and access privileges are restricted accordingly.

The USDA e-Auth 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 experts in such matters.

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 if the user has access to the system. Access must be warranted based on user position and status as an employee with FSIS.

In FIMS, no accounts are deleted; they are marked inactive. The employee's phone number and e-mail remain. The phone number is the only PII left in the system.

The incident information is stored and retained after the incident is resolved, and is utilized for trend analysis.

The data from the HR-GSS DB will be maintained long term for reporting.

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

Yes, DAA-0584-2015-003 Request for Records Disposition Authority was approved. FSIS also 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.

The following data is shared internally by facilities within the Mission Area, including PHIS, HR-GSS, and ANet.

Table 4-1: Data Shared by Internal Mission Areas

Mission Area Boundary Data Received From	List the purpose of the Data Received	List of Specific Data Element Types Received	Method of Transmittal	Provide name of Applicable Area Sites
PHIS	Meat Company of the Incident Report in FIMS	Under the General heading: Establishment Number, Name, City, State, Estimated Size, and Fed/TA/ST Est. Under the Slaughter Volume heading: Meat, Poultry, and Other. Under the Processing Volume: Meat, Poultry, Egg Product, RTE, and Other	This data is pulled by using an API data call by FIMS.	Azure
HR-GSS	To create an Employee Absenteeism Tracker for FIMS offices to keep track of their employee's illnesses, when tornadoes hit the areas, etc. (See **Example:** in Section 1.1 above.)	Roster_Dutystation Table: Fields: state, county, city, code. Roster_Officelevel2, short_name, code. Roster_Federalemployee Table: Fields: empowhr_id. Roster_Ohrpemployee Table: Fields: first_name, middle_name, last_name. Staffing_Establishment Table:	The data originating from the HR-GSS tables/fields will be pulled from within the PostGresSQL database (DB) server maintained in Digital Infrastructure Services Center (DISC) Platform as a Service (PaaS) tables/fields. FIMS will run queries, through an	DISC in Kansas City, MO.

Mission Area Boundary Data Received From	List the purpose of the Data Received	List of Specific Data Element Types Received	Method of Transmittal	Provide name of Applicable Area Sites
		Fields: est_num, est_name, est_city, est_state, est_zip.	API, against the larger HR-GSS dataset. FIMS will then receive the data originating from those HR-GSS tables/fields as input. FIMS will store that data in its PostGresSQL DB server maintained in DISC PaaS.	
ANet	Unique & Distributer, Inc., of the Incident Report in FIMS	Under the General heading: Firm ID#, Tier, Warehouse Name, City, and State	This data is pulled by using an API data call by FIMS.	Azure

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.

To have a FIMS account, the user must enter their contact information including first and last name, personal cell phone, home phone, smart phone number, FSIS desk phone, and FSIS e-mail addresses. Therefore, the risk is low that a user might share their personal contact data with another user, or 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 defense incidents appropriately and that requires sharing of some contact information, such as name, work phone, and/or e-mail. The explicit intent of the system is to enable quick and effective response through the sharing of incident 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 organizations external to the USDA.

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.

FIMS does not share PII outside of the Department.

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

The United States does not have a single overarching data protection law beyond the provisions of HIPAA and other legislation pertaining to healthcare.

Therefore, *should* FIMS information ever need to be shared externally, FIMS would follow all industry-specific guidelines and requirements for providing information to external organizations.

The following are a list of those industry-specific guidelines and requirements:

- *Federal Information Security Management Act (FISMA)*
- *North American Electric Reliability Corp. (NERC) standards*
- *Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *The Health Information Technology for Economic and Clinical Health Act (HITECH)*
- *Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule)*
- H.R. 2868: *The Chemical Facility Anti-Terrorism Standards Regulation*.

This includes the redacting of PII, unless the information is required under law.

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

If employee PII data is transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee PII 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 Does this system require a SORN and if so, please provide SORN name and URL.

FIMS is leveraging the PHIS, ANet, and HR-GSS SORNs.

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

Yes. Notice is provided to the individual prior to collection of any information, in accordance with USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII) for all Source System users. Plant vendors are provided notification during business agreement processes.

The user is told prior to system access that entering their name is a requirement of working on the system; therefore, the user is notified.

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

No. Because collection of the information is a requirement to access FIMS, if they decline, they cannot work on the FIMS system.

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

No.

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

The user is told prior to system access that entering their name is a requirement of working on the system; therefore, the user is notified.

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?

Individuals with FIMS access can access and update their contact information at any time on their employee personal page within the FIMS system. Additionally, individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA office.

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 2166, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 720-2109 - Fax (202) 690-3023 – E-mail: fsis.foia@usda.gov.

For more information about how to make a FOIA request, please see:

http://www.fsis.usda.gov/wps/portal/footer/policies-and-links/freedom-of-information-act/foia-requests

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

Individuals with FIMS access have the ability to update their personal information on their personal page. Additionally, the individual wishing to correct inaccurate or erroneous information should contact the system owner.

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

Before providing information, the individual is presented with a Privacy Act Notice and an explanation of the Notice, on both the USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII).

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

N/A. Formal redress is provided. See 7.2 above.

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 approvals. Users must have e-Auth access and must be approved for access to FIMS by the FIMS team in FSIS' Office of Management. 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 experts 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 are required in their jobs to handle sensitive and confidential information.

8.4 Has Assessment & Authorization been completed for the system or systems supporting the program?

Yes. The Authority to Operate (ATO) was granted on 05/25/2021.

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 executive assistant roles can update their supervisors' information.

FIMS also has activity audit capabilities using three separate reports.

FIMS has the following technical safeguards are in place:

- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS 201, *Personal Identity Verification (PIV)*

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*
- Cybersecurity and Infrastructure Security Agency (CISA) *High Value Asset Control Overlay, Version 2.0, dated January 2021*.

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 eAuth 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"?

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

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.

If so, is it done automatically?

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

If so, is it done on a recurring basis?

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?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

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.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

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

Lucy Touhey
System Owner (SO)
1400 Independence Ave, SW
South Building
Room 2129
Washington, DC 20472

Marvin Lykes
Chief Information Security Officer (CISO)
1400 Independence Ave., SW
Washington, DC 20250

Carl A. Mayes
Chief Information Officer (CIO)
1400 Independence Ave., SW
Washington, DC 20250

Approval Signatures

LUCY TOUHEY Digitally signed by LUCY TOUHEY
Date: 2023.07.11 07:12:55 -04'00'

Lucy Touhey
System Owner

DATE

MARVIN LYKES Digitally signed by MARVIN LYKES
Date: 2023.07.12 09:43:03 -04'00'

Marvin Lykes
FSIS Chief Information Security Officer (CISO)

DATE

CARL MAYES Digitally signed by CARL MAYES
Date: 2023.07.12 10:23:54 -04'00'

Carl A. Mayes
FSIS Assistant Chief Information Officer

DATE