U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 10.1

OFFICE OF THE CHIEF PRIVACY OFFICER

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement, PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

FSIS Incident Management System (FIMS)

Food Safety and Inspection Service (FSIS)

Office of Management (OM)

Date PIA submitted for review:

March 4, 2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Timothy Poe	Timothy.Poe@usda.gov	(202) 937-4207
Information System Security Manager	Marvin Lykes	Marvin.Lykes@usda.gov	(202) 515-6115
System Owner	Lucy Touhey	Lucy.Touhey@usda.gov	(202) 309-2607

Abstract

Food Safety and Inspection Service (FSIS) Incident Management System (FIMS) is a containerized application hosted on Linux RHEL in the Microsoft Azure Cloud Platform as a Service (PaaS) located in Virginia and a secondary site in Texas. The purpose of the FIMS system is to monitor the receipt and follow-up actions on all Incident Reports (IRs) received by the agency, and to enhance communications among FSIS offices through automated workflows, and communication lines, such as e-mail and phone. FIMS collects the user's contact information including first and last name, personal cell phone, home phone, FSIS cell phone, and FSIS e-mail addresses. This information is mandatory to work on FIMS, and the user is required to input into My Page themselves, but is not used in incident responses. A PIA is required because the system uses Personally Identifiable Information.

Overview

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 original launch. FIMS includes features such as Geographical Information Services (GIS) mapping, management of Incident Reports (IRs) and the Emergency Management Committee (EMC), and individual profiles.

- FIMS is owned and managed by the Office of Management.
- The system is not used in any other sites, other than the Azure environment, under the FSIS.
- FIMS supports and manages all food related incidents within processing plants, and other meat, poultry, and egg establishments.
- FIMS currently has approximately 100 users at this time.
- FIMS 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/Senior Executive Duty Officer (SEDO), and Executive Manager. Some of these roles may be able to perform the following tasks:
    1. Managing users within the system
    2. Creating/updating the information related to IRs
    3. 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.

Section 1.0 Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

Generally speaking, the authorities for USDA to collect, maintain, use and disseminate information 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).

Regarding the authorities that allow the USDA to collect information described herein this document, the 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).

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).*

1.2 Has Authorization and Accreditation (A&A) been completed for the system?

Yes. The last FIMS ATO letter is dated 05/25/2021. FIMS is currently undergoing its ATO assessment.

FIMS has been classified as a Moderate system according to FIPS 199.

1.2. What System of Records Notice(s) (SORN(s)) apply to the information?

N/A, PII is not retrieved by a personal identifier.

1.4. Is the collection of information covered by the Paperwork Reduction Act?

No.

Section 2.0 Characterization of the Information

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

2.1. What information is collected, used, disseminated, or maintained in the system/program?

FIMS collects the user's contact information including first and last name, personal cell phone, home phone, FSIS cell phone, and FSIS e-mail addresses. This information is required to be input into My Page to be able to work on FIMS, however, information is not retrieved by a personal identifier. Furthermore, the user PII is not used in incident responses, or in any other way, except to be able to work on the system.

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, and 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.

Identifying Numbers			
☐	Social Security number	☐	Truncated or Partial Social Security number
☐	Driver's License Number	☐	License Plate Number
☐	Registration Number	☐	File/Case ID Number
☐	Student ID Number	☐	Federal Student Aid Number
☐	Passport number	☐	Alien Registration Number
☐	DOD ID Number	☐	DOD Benefits Number
☐	Employee Identification Number	☐	Professional License Number
☐	Taxpayer Identification Number	☐	Business Taxpayer Identification Number (sole proprietor)
☐	Credit/Debit Card Number	☐	Business Credit Card Number (sole proprietor)
☐	Vehicle Identification Number	☐	Business Vehicle Identification Number (sole proprietor)
☐	Personal Bank Account Number	☐	Business Bank Account Number (sole proprietor)
☐	Personal Device Identifiers or Serial Numbers	☐	Business device identifiers or serial numbers (sole proprietor)
☒	Personal Mobile Number	☒	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number		
Biographical Information			

☒	Name (including nicknames)	□	Gender	□	Business Mailing Address (sole proprietor)
□	Date of Birth (MM/DD/YY)	□	Ethnicity	□	Business Phone or Fax Number (sole proprietor)
□	Country of Birth	□	City or County of Birth	□	Group/Organization Membership
□	Citizenship	□	Immigration Status	□	Religion/Religious Preference
□	Home Address	□	Zip Code	☒	Home Phone or Fax Number
□	Spouse Information	□	Sexual Orientation	□	Children Information
□	Marital Status	□	Military Service Information	□	Mother's Maiden Name
□	Race	□	Nationality	□	Global Positioning System (GPS)/Location Data
□	Personal e-mail address	☒	Business e-mail address	□	Personal Financial Information (including loan information)
□	Employment Information	□	Alias (username/screenname)	□	Business Financial Information (including loan information)
□	Education Information	□	Resume or curriculum vitae	□	Professional/personal references
Biometrics/Distinguishing Features/Characteristics					
□	Fingerprints	□	Palm prints	□	Vascular scans
□	Retina/Iris Scans	□	Dental Profile	□	Scars, marks, tattoos
□	Hair Color	□	Eye Color	□	Height
□	Video recording	□	Photos	□	Voice/ Audio Recording
□	DNA Sample or Profile	□	Signatures	□	Weight
Medical/Emergency Information					
□	Medical/Health Information	□	Mental Health Information	□	Disability Information
□	Workers' Compensation Information	□	Patient ID Number	□	Emergency Contact Information
Device Information					
□	Device settings or preferences (e.g., security level, sharing options, ringtones)	□	Cell tower records (e.g., logs, user location, time, etc.)	□	Network communications data
Specific Information/File Types					
□	Personnel Files	□	Law Enforcement Information	□	Credit History Information
□	Health Information	□	Academic/Professional Background Information	□	Civil/Criminal History Information/Police Record
□	Case files	□	Security Clearance/Background Check	□	Taxpayer Information/Tax Return Information

2.2. What are the sources of the information in the system/program?

The source of the information are the FIMS users, themselves, as well as individuals reporting an incident at an establishment.

2.2.1. How is the information collected?

The information is collected by the FIMS users, themselves. 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.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

No.

2.4. How will the information be checked for accuracy? How often will it be checked?

FSIS users are responsible for the accuracy of the information they enter on My Page, as well as incident information. Additionally, system Administrators ensure the FIMS system is accurate and up-to-date.

2.5. Does the system/program use third-party websites?

No

2.5.1. What is the purpose of the use of third-party websites?

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

2.5.1.1. What PII will be made available to the agency though the use of third-party websites?

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

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

Follow the format below:

Privacy Risk: There is a risk that FIMS collects too much information from users.
Mitigation: This risk is mitigated because FIMS only collects the user's contact information including first and last name, personal cell phone, home phone, FSIS cell phone, and FSIS e-mail address to monitor the receipt and follow-up actions on all Incident Reports (IRs) received

by the agency, and to enhance communications among FSIS offices through automated workflows, and communication lines, such as e-mail and phone.

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.

Section 3.0 Uses of the Information

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

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

User information on My Page is used for access to the FIMS application, 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.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No. There are no tools used to analyze the IR data. Data is produced through IR generation.

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

Follow the format below:

Privacy Risk: There is a risk that information in the system could be used for unintended purposes or accessed by unauthorized users.

Mitigation: This risk is mitigated because 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 also 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., Software 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 4.0 Notice

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

4.1. How does the project/program/system provide notice to individuals prior to collection?

Notice is provided to the individual when they go to the site to register for their account. Once there, the individual will go to the FIMS application for the first time and complete the enrollment. Part of the process is a screen that explains the privacy notice in accordance with USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII) for all Source System individuals. Once the individual clicks the button to acknowledge receiving, reading, and understanding the Privacy Notice, it then moves the individual to the FIMS consent policy, explaining the individual must consent to creating the My Page with their first and last name, personal cell phone, home phone, FSIS cell phone, and FSIS e-mail address, as this is a requirement of working on the system. If the individual agrees, they click a button acknowledging they received, read, and understand the policy, and will be taken to the My Page for inserting those fields. If the individual declines, the system will close, and the individual cannot work on FIMS without agreeing to create a FIMS My Page with their PII.

4.2. What options are available for individuals to consent, decline, or opt out of the project?

Users have the option to not submit an application for access to the system. However, users who decline to submit an application will not be able to work on the FIMS system.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

Privacy Risk: There is a risk that individuals could be unaware of the scope of information collected and not understand how to opt out of participation.

Mitigation: This risk is mitigated. At the Registration site, individuals are shown the Privacy Notice and the consent policies on a screen, and the individual must click a button to acknowledge they received, read, and agree to them.

The individual either agrees to receiving, reading, and acknowledging both the Privacy Notice and the FIMS Consent policy by clicking the button, or they do not agree and the system will close.

Section 5.0 Data Retention

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

5.1. What information is retained and for how long?

Contact information which includes users first and last name, home and business phone numbers, and business email addresses is retained while the user has access to the system. When a user ends employment with FIMS, the first and last name, and personal phone numbers are deleted, and the account is marked inactive. When user accounts are marked inactive, only the employee's FSIS business number and e-mail address remain in the system indefinitely.

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

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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.

5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information.

Follow the format below:

Privacy Risk: There is a risk that information may be misused since business e-mail addresses contain employee first and last names and remain in the system after employment ends.

Mitigation: This risk is partially mitigated by granting access only to authorized persons. All USDA employees have undergone a background investigation, and all FSIS employees must complete the annual security awareness training to maintain FSIS computer network account access.
Access to computerized files is also password-protected and under the direct supervision of the system manager. The system manager has the capability of auditing access from the computer media, thereby permitting regular ad-hoc monitoring of computer usage.

Section 6.0 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

FIMS data is not shared internally.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

N/A

6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Information is not shared with organizations external to the USDA.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

N/A

Section 7.0 Redress

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

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 no longer have access to the system can submit a Freedom of Information Act request to:

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. All user PII is on that page and users control accuracy.

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

Notice is generally given in the registration process that empowers the user to correct their data and maintain accuracy.

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

N/A.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk: There is a risk that users may not know how to gain access to their information to correct or update it.

Mitigation: This risk is mitigated. Individuals with FIMS access have the ability to update their personal information on their personal page. All user PII is on that page and users control accuracy.

Section 8 Auditing and Accountability

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

8.1. How is the information in the system/project/program secured?

Access to the system is controlled by the e-Authentication (e-Auth) 2.0 system, which is standard for all USDA Web-based applications, according to Office of the Chief Information Officer (OCIO) Department Regulation 3610-001, *USDA e-Authentication Service.*

Information is secured through the USDA-approved secure single sign-on application. The e-Auth level of enforcement for FIMS is currently Level 2.
All users, including the System and Database Administrators will access FIMS after logging into e-Auth. The user will use their e-Auth authenticators to log into the FIMS system.

The FIMS system is a Web-based client/server application that lives in the USDA's intranet; it implements e-Auth 2.0 for authorizing users and granting access to the system's functionalities.

Access and authorization within FIMS are role-based to ensure least privileges.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

FIMS is role-based to ensure least privileges and this is documented through the USDA Departmental Manuals.

8.3. How does the program review and approve information sharing requirements?

There is no information sharing requirements on FIMS, as FIMS does not share information outside of the USDA.

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

The USDA AgLearn provides privacy training through their online training courses. The USDA maintains all the Department's employee's training certificates.

Approval Signatures:

____

Lucy Touhey
Food Safety and Inspection Service (FSIS)
Office of Management (OM)
United States Department of Agriculture

____

Timothy Poe
Privacy Officer
Food Safety and Inspection Service
United States Department of Agriculture

____

Marvin A. Lykes
Security Compliance & Infrastructure Operations Center
Office of the Chief Information Officer
Food Safety and Inspection Service
United States Department of Agriculture

____

David Lindner
Chief Privacy Officer
United States Department of Agriculture