USDA Privacy Impact Assessment

Fiscal Year 2025

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”
08/05/2025	1.2	Updated with latest information.

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Farm Service Information Management System (FSIMS)
Program Office	Information Solutions Division
Mission Area	Farm Program and Conservation – Business Center (FPAC-BC)
CSAM Number	1322
Date Submitted for Review	-

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Samantha Jones	202-221-9289
Information System Security Manager	Karl Hill	816-823-1496
System/Program Managers	Laurie Sigman Nancy Dudley	816-926-1472 816-926-6298

Abstract

The Farm Service Information Management System (FSIMS) supports USDA FPAC to efficiently store, organize and manage large amounts of information, which can be used for auditing, analysis and reporting purposes. The programs ingest and stores data within a data lake in a format which is searchable and usable for analytics, data calls, and reporting. FSIMS uses the information collected to store, organize and manage large amounts of information. This information can be used for auditing, analysis, and reporting issues. The PIA is being conducted because this system contains PII.

Overview

FSIMS is owned by the Information Solutions Division within USDA's Farm Production and Conservation Business Center (FPAC-BC). The business purpose of the information technology (IT) system is to efficiently store, organize and manage large amounts of information so that information can be used for auditing, analysis, and reporting issues. This relates to FPAC-BC's de mission to provide support across 15 business lines, such as budgeting, civil, and human resources, for Farm Service Agency (FSA), Natural Resources and Conservation Service (NRCS), and Risk Management Agency (RMA).

The system, which users include approved FPAC business, was created to provide timely access to quality information and to establish, enhance, and maintain the automated processes for gathering, accessing, and analyzing data in support of helping enterprise users make informed business decisions. The program provides business users with a single source for data used to resolve business inquiries.

It is estimated that approximately 20 million users' information is stored within the Enterprise Data Warehouse. The consolidated data warehouse provides information to FPAC national, state, and county personnel. The Enterprise Data Warehouse is designed to facilitate data retrieval and reporting by providing a central stable location for data storage across FSA's business enterprise FSIMS consists of 4 applications, which include (1) Enterprise Data Warehouse (RedShift), (2) Legacy Informix Reporting Systems (INFOR), and (3) AWS Simple Storage (S3), (4) PostGres Database (Monitoring & RDS). The applications house the migrated and new data marts, serve as the data repository for information that supports several reporting and analysis needs within FPAC, and support customer reporting needs.

The legal authorities to operate the IT system include the Commodity Credit Corporation Charter Act** (15 USC 714 et seq.). The completion of this PIA will not result in changes to business processes or technological changes.

Section 1: Authorities and Other Requirements

These questions identify all statutory and regulatory authorities for operating the project, application, or system, including the authority for collection, which SORN applies, if an ATO has been completed, and if there is Paperwork Reduction Act coverage:

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

The legal authority to permit the collection of information by FSIMS the Commodity Credit Corporation Charter Act (15 U.S.C. 714 et seq.) and Executive Order 9397.

Has Authorization and Accreditation (A&A) been completed for the project, application, or system?

- Security Plan Status: Completed
- Security Plan Status Date: April 17, 2024
- Authorization Status: Authorized To Operate
- Authorization Status Date: April 17, 2024
- Authorization Termination Date: April 17, 2027
- Risk Review Completion Date: March 28, 2024
- FTPS 199 Classification of the System: Moderate

Which System of Records Notices (SORNs) apply to the information?

The following SORNs cover FSIMS: FSA-2 and FSA-14 in Federal Register Vol. 84, No. 56

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

No

Section 2: Information Characterization

These questions define the scope of the information requested and collected, as well as the reasons for its collection as part of the project, application, or system being developed:

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

Identifying Numbers:

- Truncated or Partial Social Security Number
- Driver's License Number
- Passport Number
- Employee Identification Number
- Taxpayer Identification Number

Biographical Information:

- Name (Including Nicknames)
- Business Mailing Address (Sole Proprietor)
- Date of Birth
- City or County of Birth
- Home Address
- ZIP Code
- Employment Information
- Business Financial Information (Including Loan Information)

What are the sources of the information in the project, application, or system?

The EDW will extract transform and load information from multiple SAP source systems including Farm Program Business Partner and Farm Records System (MIDAS), Web-Based Supply Chain Management (WBSCM) and Financial Management Modernization Initiative (FMMI), as well as non-SAP systems, such as Farm Records, GIS, Eligibility, and financial data from SQL Server systems.

How is the information collected?

Most PII data collected from the producer at the county office and entered by the county office staff. In some cases, information is collected via other federal agencies which provide this information to the FPAC. This data resides in multiple source systems and is extracted from the source systems into the EDW.

Does the project, application, or system use information from commercial sources or publicly available data? If so, explain why it is used.

No

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

Data collected from the producer is checked by the county office official entering the data. There are also data profiling efforts to verify the accuracy of the data after it is entered into the source system.

Does the project, application, or system use third-party websites?

No

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

N/A

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

N/A

List the privacy risks and mitigations related to the characterization of the information.

Privacy Risk: The information collected contains sensitive PII, which if disclosed, would cause an unwarranted invasion of personal privacy.

Mitigation: The information is only disclosed to those responsible for the administration of the program or other entities that have legal authority to access the information. Users are required to authenticate their identity prior to accessing the information and access is restricted based upon user role.

Section 3: Information Uses

These questions delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated and/or maintained will support the project, application, or system's business purpose.

The information is being collected to meet the reporting needs of the agency and comply with federal regulations and legislative mandates.

Most PII data collected from the producer at the county office and entered by the county office staff. In some cases, information is collected via other federal agencies which provide this information to the FSA. This data resides in multiple source systems and is extracted from the source systems into the EDW.

Does the project, application, or system 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.

Oracle Analytics Server (OAS) and Tableau will be used to analyze the data. Data related to farms, producers, crops, and commodities which will be used to meet congressional reporting requirements along with ensuring compliance to federal regulations.

List the privacy risks and mitigations related to uses of the information.

Privacy Risk: Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Mitigation: All users must be uniquely identified and authenticated using FSA Form 13A process prior to accessing the application. Access to data is restricted and access to the system and data are determined by business need and individual roles.

Section 4: Notice

These questions are intended to provide notice to the individual of the scope of information collected, the right to consent to use of the information, and the right to decline to provide information.

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

Privacy Act Statements are placed on each form that collects PII. The statement notifies the individual of the authority to collect the information, what organizations may be legally authorized to receive it, how the information may be used, and individual's option to refuse to provide the information to USDA.

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

Individuals may decline to provide any of the information without penalty. However, refusing to provide some information could delay processing or result in the denial of their application. Users have the right to provide consent to access their information. To do so, the individual must make a written request to the information owner, system owner, or Privacy Officer to evaluate their request.

List the privacy risks and mitigations related to notice.

Privacy Risk: Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Mitigation: The information collected in accordance with USDA SORN FSA-2 and FSA-14 is a part of a Privacy Act System of Records that requires safeguarding access and disclosure when legal authority exists. The system information is specific to each individual and could cause moderate harm to individuals upon unauthorized disclosure. As a result of the information being connected to USDA SORN FSA-2 and FSA-14 information in the system can be only accessed or disclosed upon legal authority or dictated routine use.

Section 5: Data Retention

These questions outline how long information will be retained after the initial collection.

What information is retained and for how long?

All records found in FSIMS are retained for 10 years and deleted only after the information is no longer needed for administrative, legal, audit or other operational purposes.

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

The retention schedule has been approved by the USDA records office and NARA. The Records Schedule Numbers are DAA-0145-2018-0003 & DAA-0145-2015-0014-0004.

List the privacy risks and mitigations related to data retention.

Privacy Risk: The information contained in the records are sensitive, which could cause a privacy breach if not properly safeguarded.

Mitigation: Access and destruction of the information will only occur upon establishment of proper legal authority to access the data, pursuant the Privacy Act, Section 1619 of the Farm Bill, and the appropriate SORN(s) covering the information.

Section 6: Information Sharing

These questions define the content, scope, and authority for information sharing.

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

FSA source systems (not EDW) share PII with NRCS, RD, and RMA. FSA source systems shares information through batch processes.

List the privacy risks and mitigations related to internal information sharing and disclosure.

Privacy Risk: Unauthorized access to sensitive data could pose a risk to existing data and disclosure to unauthorized parties.

Mitigation: Information is electronic transmission of the data is encrypted, and access is only granted based on a user's role and active/inactive status.

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

EDW does not directly share information with external entities; However, FSA shares with IRS Treasury, one time data share with the University of Illinois, Dunn and Bradstreet (Name and address validation).

List the privacy risks and mitigations related to external information sharing and disclosure.

Privacy Risk: The information collected in accordance with SORN FSA-2 and FSA-14 is part of a Privacy Act System of Records that requires safeguarding, access and disclosure when legal authority exists. The system information is specific to each individual and could cause moderate harm to the individual upon unauthorized disclosure.

Mitigation: As a result of the information being part of SORN FSA-2 and FSA-14 information in the system can be only accessed or disclosed upon legal authority or routine use.

Section 7: Redress

These questions address the individual's ability to ensure the accuracy of the information collected about him or her.

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

Should an individual wish to gain access to their information, they will need to make a written request to the system owner or FPAC FOIA Officer, to authenticate their identity and identity the records they request access to FSIMS.

What are the procedures for correcting inaccurate or erroneous information?

Individuals must make a written request to the system owner, information system owner or Privacy Officer, authenticate their identity, identify the portion(s) of the record that needs to be corrected and describe whether their information is inaccurate or erroneous. Upon receipt and review of the request, if it is verified a correction needs to be made, the record will be corrected and a sample of the document with the correction will be transmitted to the individual who made the request.

Requests to correct a record should be sent directly a local or state FSA Office. All requests (1) must be in writing, (2) clearly identify the information that needs correction, (3) provide a reason why the information is incorrect, and (4) state what the correction should be.

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

In addition to normal notification through the SORN process, field technicians provide correction procedures to individuals upon request.

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

Individuals may contact their administrative point of contact to obtain access to their information.

List the privacy risks and mitigations related to redress.

Privacy Risk: The system information provided by participants is important to be accurate, as it has an impact on their program participation. Incorrect information may adversely affect the participant or other individuals, result in denial of service or incorrect payments.

Mitigation: Individuals are provided with access to their information electronically to check for accuracy of their submission(s). Additionally, program staff will verify submitted information with the individual as well as previously collected data.

Section 8: Auditing and Accountability

These questions describe technical safeguards and security measures:

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

USDA eAuthentication is the system used by USDA agencies to enable customers and employees to obtain accounts that will allow them to access USDA Web applications and services via the Internet. This includes things such as submitting forms electronically, completing surveys online, and checking the status of your USDA accounts. Please note that USDA will only accept eAuthentication Accounts from individuals. Currently USDA eAuthentication does not have the mechanism to issue accounts to businesses, corporations or other entities.

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

Access to PII is determined by user role and restricted access. Access to PII is granted by appropriate legal authorities. Applicable user and roles are documented in the System Security Plan.

How does the program review and approve information sharing requirements?

Any time organizations outside of USDA requests access to information, a data sharing agreement is created and routed through the Grants and Agreements Office for review. The Grants and Agreements Office ensures all stakeholders, to include, but not limited to the FPAC Privacy Officer, a Senior Agency Official, and receiving organization official, review and sign the data sharing agreement that lays forth the standards and rules for handling USDA PII.

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

Annual organizational training, including USDA Information Security Awareness Training & Acknowledgment of Rules of Behavior, is mandatory for all federal and contractor staff working with FSIMS.