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.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Farm Program Common Management System (FPCMS)
Program Office	Common Processes Branch
Mission Area	Farm Production and Conservation (FPAC)/ Farm Service Agency (FSA)
CSAM Number	1289
Date Submitted for Review	6/10/2025

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	Alexandra Carson Justin Horn Suman Sarekukka	816-994-4512 816-823-1584 816-823-2949

Abstract

Farm Program Common Management System (FPCMS) supports various FSA farm programs by providing common information to automated systems related to County Offices, specific farm crops, and various farm programs. FPCMS uses the information collected to provide common customer and farm details, which are used to validate eligibility for participation in supported programs listed above. The PIA is being conducted because this system contains PII.

Overview

Farm Program Common Management System (FPCMS) is owned by the Program Delivery Division (PDD) within USDA's Farm Service Agency (FSA). The business purpose of the information technology (IT) system is to provide common customer and farm information that is used to validate eligibility for participation in FSA programs. This relates FSA's mission to serve farmers ranchers, and agricultural partners through the delivery of effective, efficient agricultural programs for all Americans.

The system, which users include FSA and NRCS headquarters and field employees was created to provide a common platform for managing various farm programs, including those administered by the FSA.

It is estimated that approximately 14 million customers' information is stored within FPCMS. FPCMS is currently comprised of 6 applications which include (1) Common Payment Program (CPP), (2) Common Selection (COMSEL), (3) Compliance Query Tool (CQT), (4) Payment to Producers Identified as Deceased (PPID), (5) Service Center Information Management System (SCIMS), (6) Subsidiary Systems (Subsid). The applications provide the following purposes:

- Contain common processes for payments for all program applications
- Provide consistent, standardized selection of Farm Program applications based on common parameters
- Assists State and County Offices in conducting reviews and recording the results of the reviews for the Payments to Producers Identified as Deceased Report
- Provide an interface for the Service Center Agencies and its customers to view customer data in a centralized data repository (SCIMS is read-only for all users)
- Maintain combined producers, multiple county producers, payment limitation, and producer eligibility for use in controlling producer payments and participation in FSA Farm Programs.

The legal authority to operate the IT system includes 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 FPCMS is the Commodity Credit Corporation Charter Act** (15 USC 714 et seq.).

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

- Security Plan Status: Completed. New Security Plan underway
- Security Plan Status Date: September 16, 2024
- Authorization Status: Authorized to Operate
- Authorization Status Date: September 16, 2024
- Authorization Termination Date: September 16, 2027
- Risk Review Completion Date: July 15, 2024
- FTPS 199 Classification of the System: Moderate

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

The following SORNs cover FPCMS:

- FSA-2 SORN in Federal Register Vol. 84, No. 56, Friday, March 22, 2019
- FSA-14 SORN in Federal Register Vol. 84, No. 56, Friday, March 22, 2019

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:

- Social Security Number
- Truncated or Partial Social Security Number
- Employee Identification Number
- Taxpayer Identification Number
- Business Taxpayer Identification Number (Sole Proprietor)
- Personal Mobile Phone Number
- Business Mobile Phone Number (Sole Proprietor)

Biographical Information:

- Name (Including Nicknames)
- Business Mailing Address (Sole Proprietor)
- Date of Birth
- Ethnicity
- Business Phone or Fax Number (Sole Proprietor)
- Country of Birth
- City or County of Birth
- Citizenship
- Home Phone or Fax Number
- Home Address
- ZIP Code
- Marital Status
- Spouse Information
- Race
- Nationality
- Personal Email Address
- Business Email Address

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

The information is supplied directly from producers, on a voluntary basis via OMB-approved forms.

How is the information collected?

Information is collected from producers on OMB-approved forms, and then manually entered into systems by authorized program staff.

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 customer is required by policy to be reviewed for accuracy, relevancy, timeliness, and completeness upon initial entry into the system and then again when any required updates are made.

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

No

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

No

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: Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Mitigation: Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

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 collected is used to support USDA program implementation to provide common customer and farm details, which are used to validate eligibility for participation from supported programs. Information is manually entered by program support staff in source systems.

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.

No

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

Privacy Risk: Access to the data collected must be monitored to ensure safeguarding against unauthorized access and use.

Mitigation: Access to PII is determined by the owner of the information, user roles, and restricted access. Additionally, access will only be granted to the PII upon appropriate legal authority.

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 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. USDA Customers 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.

Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Mitigation: Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

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?

Some records found in FPCMS are retained indefinitely and deleted or archived 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 Number is DAA-0145·201NI01B and DAA-0145-2017-0018-0002.

List the privacy risks and mitigations related to data retention.

Privacy Risk: Excessive Data Retention: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

Data Breaches: The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Mitigation: Data Retention Policy: Use NARA data retention policies that outline how long different types of PII will be retained and the rationale for those timeframes.

Regular Reviews: Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.

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?

Over 130 calling applications use SCIMS shared service to utilize data in many different capacities. Many of these are NRCS or FSA applications. Cooperative Interstate Shipment (CIS) application also uses shared services. PII information such as SSN/Tax IDs, DOB and addresses are securely transmitted through the shared service to help facilitate processes such payments or report generation.

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?

None

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

Privacy Risk: N/A

Mitigation: N/A

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, an approved OMB form must be completed and submitted to the county office staff to authenticate their identity and identity the records they request access to FPCMS.

What are the procedures for correcting inaccurate or erroneous information?

Individuals must make a written request to the county office staff, usually on an approved OMB form requesting the changes or correction 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 to 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, resulting 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?

The FPCMS employs a defense-in-depth strategy. Web applications are protected by web application firewall and restrictive networking. The application server is configured using Center for Internet Security hardened images and all components employ end point protection and real-time monitoring for malicious activity. Access to the system is role-based and requires multi-factor authentication for all accounts. All data transfer and storage utilize Federal Information Processing Standard (FIPS 140-2) compliant encryption.

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 ensure 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 FPCMS.