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 Service Program Compliance System (FSPCS)
Program Office	Internal Auditing Branch
Mission Area	Farm Production and Conservation – Business Center (FPAC-Business Center)
CSAM Number	2385
Date Submitted for Review	6/13/2025

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	Rani Agnihotri	202-690-0458

Abstract

The Farm Service Program Compliance System (FSPCS) supports USDA's various FPAC-BC programs. The FPAC-BC combines the talent of employees from all three FPAC agencies into specialized teams that serve employees and customers across the Farm Service Agency (FSA), the Natural Resource Conservation Service (NRCS), and the Risk Management Agency (RMA). This new business approach helps agencies improve operations and efficiency at USDA and boosts support for America's farmers, ranchers and foresters. FSCPS uses the information collected to facilitate the evaluation of internal controls at the National, State, and County levels. The PIA is being conducted because this system contains PII.

Overview

FSPCS is owned by the Internal Auditing Branch within USDA's FPAC-BC. The business purpose of the information technology (IT) system is to facilitate the evaluation of internal controls at the National, State, and County levels. This relates to FPAC-BC mission to provide enterprise solutions for mission support activities including information technology, financial management, human resources, acquisition, property management, and related business and administrative processes to improve customer service at the mission area level. The system was created to enable internal reviews of County Office operations, provide the ability to monitor compliance to actions identified by Office of the Inspector General (OIG), General Administrative Office (GAO) and other FSA reporting parties, and facilitate compliance of Payment Integrity Information Act which requires federal agencies to implement financial management controls that prevent improper payments. FPAC-BC programs assist FSA, FBC, NRCS, and FSA agencies in internal audit reviews for National, State, and County levels.

It is estimated that information of approximately 40,000 individuals is stored within FSPCS. The information collection includes improper payments, tracking of correspondence related to the legal, business, and personnel practices at USDA and the ability to review County level operations and practices to ensure program delivery matches program policy. FSCPS is currently comprised of three applications, which include (1) Electronic County Operations Review Program (eCORP), (2) Electronic Oversight Tracking System (eOTS), and (3) Improper Payments Information Act (IPIA). Information collection includes improper payments, tracking of correspondence related to the legal, business, and personnel practices at USDA and the ability to review County level operations and practices to ensure program delivery matches program policy.

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 FSPCS is the Payment Integrity Information Act (PIIA) of 2019, and the legal authority to operate the IT system includes 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: February 26, 2025
- Authorization Status: Authorized to Operate
- Authorization Status Date: August 30, 2023
- Authorization Termination Date: August 30, 2026
- Risk Review Completion Date: October 29, 2024
- FTPS 199 Classification of the System: Moderate

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

The following SORNs cover FSPCS: FSA–2 SORN and FSA-14 SORN in Federal Register Vol. 84, No. 56, March 22, 2019

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

Yes, the collection of information is covered by OMB 0560-0231.

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
- File or Case ID Number
- Taxpayer Identification Number

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

The information is supplied directly from Operations Review and Analysis Staff (ORAS).

How is the information collected?

The information is collected from ORAS. The information is reviewed, and inconsistencies are recorded in the application by the users who are typically the assigned County office reviewers.

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?

The information is checked by the ORAS upon data entry. The information is reviewed, and inconsistencies are recorded in the application by the users who are typically the assigned County office reviewers.

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

No

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

Not Applicable

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

Not Applicable

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 collected is used to facilitate the evaluation of internal controls at the National, State, and County levels. Users are required to complete USDA Form AD-2035 (USDA Minority Farm Register).

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.

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 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: Transparency: Clearly outline what personal data is being collected, the purpose of data collection, how it will be used, and who it will be shared with. As a result of the information being connected to USDA 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 FSPCS 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 Number is DAA-0145-2015-006-001.

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.

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.

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?

None

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, 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 Farm Service Program Compliance System (FSPCS).

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 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. Follow this format:

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 FSPCS 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 FSPCS.