Office of the Chief Information Officer
U.S. DEPARTMENT OF AGRICULTURE

USDA Privacy Impact Assessment

Fiscal Year 2024

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	Program Funds Control System (PFCS)
Program Office	Technology Office | Information Assurance
Mission Area	Rural Development
CSAM Number	2108
Date Submitted for Review	07/16/2025

Mission Area System/Program Contacts

Role	Name
MA Privacy Officer	Ryan Schneider
Information System Security Manager	Elinor Gallelli
System/Program Managers	Deborah Wood

Abstract

The Program Funds Control System (PFCS) is a web-based financial management system designed to consolidate and reengineer the funding controls for multiple loan programs at the Farm Service Agency (FSA) and Rural Development (RD). PFCS is used to provide tools that support the budgetary and programmatic control of loan-related funds. This PIA is required under Section 208 of the E-Government Act of 2002 since PFCS collects, processes, and disseminates Personally Identifiable Information (PII) of members of the public.

Overview

PCFS is hosted on the Digital Infrastructure Service Center (DISC) platform and used internally by authorized RD employees and contractors. Authorized RD staff access PFCS using eAuthentication. General Field Representatives (GFRs), Field Office Staffs, Program Staff, Servicing Office (SO) and Chief Financial Officer (CFO) staff, access PFCS, internally via Hyper Text Transfer Protocol Secure (HTTPS) over the USDA Local Area Network (LAN).

The Program Funds Control System (PFCS) is a web-based financial management system designed to consolidate and reengineer the funding controls for multiple loan programs at FSA and RD. As such, PFCS is designed to provide tools that support the budgetary and programmatic control of loan/grant-related funds. In addition, PFCS is designed to reduce the processing time required for approving these loans and thus improve program delivery to USDA customers. The system provides overall agency funds control through interfaces with five major loan accounting systems, allows timely implementation of new loan and grant programs, and provides timely obligation and funding data for senior program managers. The PFCS “core” is a Commercial-off-the-Shelf (COTS) package using the Oracle Federal Financials, which is Joint Financial Management Improvement Program (JFMIP)-certified and meets all basic requirements for Federal Financial Management functions. It supports multiple agencies (FSA and RD) and is designed for expansion to support other entities when approved. The system is fully compatible with USDA and RD architecture and platforms.

Section 1: 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.

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

- Consolidated Farm and Rural Development Act (7 U.S.C. 1921 et seq) and Title V of the Housing Act of 1949 as amended (42 U.S.C. 1471 et seq).
- Farm Bill 2018 (P.L. 115-334)
- Fair Credit Reporting Act, 15 USC 1681 a(f)
- Consumer Credit Protection Act, 15 USC 1601
- Equal Credit Opportunity Act, 15 USC 1691
- The Fair Debt Collection Practices Act, Pub. L 111-203, title X, 124, Stat. 2092 (2010)
- 7 CFR, section 3560, subsections 55 and 154
- USDA Departmental Regulation (DR) 3080-001
- Budget and Account Act of 1950

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

Yes, ATO expires 12/16/2025

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

RD-1 SORN, 89 FR72820, September 6, 2024

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

Yes

Section 2: 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.

What information is collected, used, disseminated, or maintained in the system/program? PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Identifying Numbers:

- File/Case ID number

Biographical Information:

- Name (including nicknames)
- Personal financial information (including loan information)

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

Information is collected from Members of the Public (U.S. Citizens) into the following sources: Commercial Loan Servicing System (CLSS), Automated Multi-Family Accounting System (AMAS), Guaranteed Loan System (GLS), Program Loan Accounting System (PLAS) and LoanSer which PFCS interfaces with.

How is the information collected?

Interfaces with the following systems: Commercial Loan Servicing System (CLSS), Automated MultiFamily Accounting System (AMAS), Guaranteed Loan System (GLS), Program Loan Accounting System (PLAS), and LoanServ. Data is transferred into PFCS by data exchange via real time or batch files.

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

No

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

Data is verified by the source systems: CLSS, AMAS, GLS, PLAS, and Loanserv users as they enter the data into those source systems.

Does the system/program 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

Privacy Impact Analysis: Related to 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.
- **Over-collection of Data**: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

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.
- **Contextual Information Use**: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.
- Risk is also mitigated with internal security and privacy controls outline in the System Security Plan. Access is limited to authorized personnel using E-Authentication. Audit logs are maintained to monitor activity. System Owners define access roles to ensure separation of duties, privileged access, and the concept of least privilege. Access to a system is requested and authorized via UAM. All users must have an eAuth Level 2 account to access PFCS

Section 3: Uses of the Information

The following questions are intended to clearly 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 program's business purpose?

PFCS collects and tracks funds appropriated by the Office of Management and Budget (OMB), which are entered into PFCS by authorized users. PFCS collects obligation and disbursement data entered from RD and FSA systems, which includes the borrower's full name and borrower ID.

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

Privacy Impact Analysis: 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.
- **Data Misuse**: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.
- **Inadequate Consent**: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Mitigation

- **Purpose Limitation**: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.
- **Data Minimization**: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.
- **User Consent**: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.
- **Transparency**: Inform individuals about how their personal information will be used, including any potential secondary uses, through clear and accessible privacy notices.
- **Regular Training**: Provide regular training for employees in privacy laws and the importance of adhering to the defined uses of personal information to ensure compliance.

Section 4: 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.

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

PFCS is not the initial source system of collection or processing of information. Notice of opportunity and/or right to decline to provide information was provided to individuals by the initial source systems prior to collection or processing of the information.

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

PFCS is not the initial source system of collection or processing of information. Consent of the individuals for use of the information would have been obtained by the initial source systems, if required, prior to collection or processing of the information.

Privacy Impact Analysis: 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.
- **Non-compliance with Regulations**: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

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.
- **User Consent**: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Section 5: Data Retention

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

What information is retained and for how long?

Accountable officers' records concerned with the accounting for, availability, and status of public funds are retained in accordance with GRS 1.1, Financial Management and Reporting Records, Item 011. These are temporary records and are destroyed when business use ceases, DAA-GRS-2013-0003-0002. Access and audit records to the system are retained in accordance with GRS 3.2, Information Systems Security Records, Item 30. These records are destroyed when business use ceases.

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, PFCS follows data retention as provided by the RD Records Management, which is in accordance with GRS 3.2, Information Systems Security Records, and Item 30.

Privacy Impact Analysis: Related to retention of information.

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.
- **Non-compliance with Regulations**: Failing to adhere to legal requirements regarding data retention periods can lead to regulatory penalties and legal liabilities.
- **Obsolescence of Data**: Retained data may become outdated or irrelevant, leading to inaccuracies in decision-making or service delivery, which can affect individuals negatively.

Mitigation

- Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.
- **Secure Disposal Procedures**: Establish secure methods for the disposal of personal information that is no longer needed, such as shredding paper documents or using data-wiping software for electronic files.

Section 6: Information Sharing

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

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?

PFCS interfaces with BI (TDW), CLSS, eServices, GLS, LoanServ, PLAS, and AMAS for reconciliation purposes such as ensuring proper budgeting and allocation of funds per loan program. The purpose of PFCS is to help collect and track funds appropriated by the Office of Management and Budget (OMB).

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk

- **Unauthorized Access**: Employees may access PII without proper clearance, leading to potential misuse.
- **Data Breaches**: Internal systems can be vulnerable to breaches, compromising PII.
- **Insider Threats**: Employees with malicious intent may exploit their access to PII for personal gain.
- **Data Misuse**: PII can be misused for purposes other than intended, leading to privacy violations.
- **Lack of Data Minimization**: Sharing excessive PII that isn't necessary for a specific task can increase exposure risk.
- **Compliance Issues**: Sharing PII without following legal and regulatory requirements can lead to penal

Mitigation

- **Access Controls**: Implement role-based access controls to limit who can access PII based on their job responsibilities.
- **Encryption**: Use encryption for data in transit and at rest to protect PII from unauthorized access.
- **Regular Training**: Provide ongoing training for employees on data privacy policies, the importance of protecting PII, and how to handle it securely.
- **Monitoring and Auditing**: Regularly monitor access logs and conduct audits to detect any unauthorized access or anomalies in data handling

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?

PFCS does not share any information with external organizations.

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: N/A

Mitigation: N/A

Section 7: Redress

The following questions are directed at an 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?

PFCS is not the initial source systems of collection or processing of their information. Individuals are notified of the procedure to gain access to their information in the Record Access Procedures section as outlined in the SORN RD-1, Record Access Procedures.

What are the procedures for correcting inaccurate or erroneous information?

PFCS is not the initial source systems of collection or processing of their information. are notified of the procedure to correct their information in the Record Access Procedures section as outlined in the SORN RD-1.

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

PFCS is not the initial source systems of collection or processing of their information. are notified of the procedure to correct their information in the Record Access Procedures section as outlined in the SORN RD-1.

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

N/A, PFCS is not the initial source system of collection or processing of their information. Redress procedures are found in the Record Access Procedures section as outlined in the SORN RD-1.

Privacy Impact Analysis: Related to redress.

Privacy Risk

- **Inadequate Processes**: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.
- **Lack of Transparency**: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Mitigation

- **Establish Clear Procedures**: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations. This is established in the listed SORN.

Section 8: Auditing and Accountability

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

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

PFCS enforces user authentication and authorization to information contained within the system prior to granting the appropriate system access based on the user's predefined access level.

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

Authentication and authorization are documented with desk procedures and approved by the PFCS system owner.

How does the program review and approve information sharing requirements?

In accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Security Guide for Interconnecting Information Technology Systems, Interconnections and ISAs are reviewed annually and will be re-signed every three years.

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

RD employees and contractors are required to undergo annual general privacy training.