Privacy Impact Assessment

Program Funds Control System (PFCS)

- Version: 2.0
- Date: June 6, 2022
- Prepared for: USDA Rural Development (RD)

United States Department of Agriculture

Privacy Impact Assessment for the Program Funds Control System (PFCS)

June 6, 2022

Contact Point

RDPrivacy@usda.gov
Rural Development, Cyber Security Division
United States Department of Agriculture

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 at the following Uniform Resource Locator (URL) address: https://pfcs.sc.egov.usda.gov:4473/OA_HTML/AppsLogin. 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 architecture and platforms.

Section 1.0 Characterization of the Information

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

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

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 data entered from RD and FSA systems, which includes the borrower's full name and borrower ID. PFCS collects disbursement data from RD and FSA systems, which included non-PII, transactional data.

1.2 What are the sources of the information in the system?

Sources of the information include Congressional appropriated funds approved by the OMB. Using the OMB-approved apportionments, USDA program staffs for FSA and RD enter allotments and allocations of funds for specific and targeted areas in PFCS. Obligation requests are entered by USDA FSA and RD employees in their respective system, such as Program Loan Accounting System (PLAS), Commercial Loan Servicing System (CLSS), LoanServ, Guaranteed Loan System (GLS), and Automated Multi-Housing Accounting System (AMAS).

1.3 Why is the information being collected, used, disseminated, or maintained?

Information is collected to consolidate and reengineer the funding controls for multiple loan programs at FSA and RD. It provides overall agency funds control through interfaces with five major loan accounting systems, allow timely implementation of new loan and grant programs, and provide timely obligation and funding data for senior program managers. The data is entered into the FSA system, PLAS, BI, CLSS, LoanServ, GLS, and AMAS systems and passed to PFCS through real time files or batch files. The employee data collected includes the system User ID for audit trail purposes

1.4 How is the information collected?

Information is collected by other source systems within the USDA, specifically PLAS, CLSS, LoanServ, FSA, GLS, and AMAS systems, and transferred into PFCS by a data exchange via real time or batch files.

1.5 How will the information be checked for accuracy?

There are many balancing processes that execute with every batch update cycle to validate the data. A PFCS reconciliation report compares the feeder system, (i.e., PLAS, CLSS, LoanServ, GLS, and AMAS) with the amounts in the PFCS system. Balancing is completed against general ledger, allotment summary, and check disbursement. The Chief Financial Officer (CFO) staff reviews these outputs daily. Data integrity controls protect the data from accidental or malicious alteration or destruction and provide assurance to the RD and FSA user that the data is valid.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Information collection in PFCS falls under the following:

- *Privacy Act of 1974, as Amended (5 USC 552a);*
- *Computer Security Act of 1987, Public Law 100-235, ss 3 (1) and (2), codified at 15 U.S.C. 272, 278 g–3, 278 g-4 and 278 h which establishes minimum security practices for Federal computer systems;*
- *OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, which establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems;*
- *Freedom of Information Act, as Amended (5 USC 552), which provides for the disclosure of information maintained by Federal agencies to the public, while allowing limited protections for privacy.*
- *Federal Information Security Modernization Act of 2014 (Pub. L. 113-283)*
- *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*
- *RD Records Management Policy – RD Instruction 2033-A*
- *NARA Records Retention – General Records Schedules*

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The privacy risk is the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the RD and FSA customer.

The PFCS system owner defines access roles to ensure separation of duties, account management and authorized access to data and information in PFCS, which is hosted on the Digital Infrastructure Services Center (DISC). Only authorized RD and FSA staff can access the PFCS application using eAuthentication (eAuth) Level 2. These measures mitigate the risks to privacy data in PFCS. PFCS is hosted in the DISC environment, which complies with all security and privacy protections required by USDA as a federal agency.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

PFCS is a tracking system for allocated program funds for PLAS, GLS, LoanServ, CLSS, and AMAS systems. Each system can then obligate available funds for program loans and grants. PFCS validates the disbursements of AMAS, PLAS, and CLSS. Funds control is required by law to prevent "anti-deficiency", which is spending more money than is appropriated by Congress. PFCS also sends data to Tabular Data Warehouse (TDW), a module in the Business Intelligence (BI) system, for reconciliation reports.

2.2 What types of tools are used to analyze data and what type of data may be produced?

A PFCS reconciliation report compares the feeder system, (PLAS, AMAS, CLSS, LoanServ, and GLS) with the amounts in the PFCS system. Balancing is completed against general ledger, allotment summary, and check disbursement. RD Chief Financial Officer (CFO) and Servicing Office reviews these outputs of obligation and loan funding data daily.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Not applicable, PFCS does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The controls in place to detect unauthorized access to PCFS information or transactions include DISC audit logs/security logs. There are logs for eAuthentication, which is how the authorized RD and FSA staff identify and authenticate to access PCFS on the DISC platform.

Section 3.0 Retention

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

3.1 How long is information retained?

All data in PFCS is permanently retained and not purged from PFCS.

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.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

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

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

PFCS data retention has the potential risk of unauthorized access, unauthorized disclosure or illegal use of the customer PII data.

The RD and FSA Finance Offices review the data daily, via loan reconciliation reports. PFCS has multiple system checkpoints in place that notify system administrators/operators verifying that eleven (11) jobs run to completion. PFCS data is stored in a secure environment behind the DISC secure mainframe infrastructure. PFCS follows the RD Records Management data retention requirements to manage risk associated with data retention.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

PFCS is an integrated system with interfaces to other internal RD applications facilitating RD funds controls for multiple loan programs at FSA and RD. It is on the RD intranet and authorized RD staff use eAuthentication to identify and authenticate before accessing PFCS.

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

4.2 How is the information transmitted or disclosed?

Information within PFCS is transmitted to the other system via HyperText Transfer Protocol Secure (HTTPS). This information shared internally within the USDA network using DISC's technical protections in place to protect the data with security and privacy protections.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The privacy risks are the unauthorized access and compromise of PII data in PFCS.

These privacy risks are mitigated by the DISC Midrange environment, which hosts the PFCS application and provides security and privacy data protection. The DISC environment complies with the USDA requirements on protecting information. Finally, only authorized RD and FSA staff access PFCS using eAuthentication (eAuth) to identify and authenticate the users. Audit logs track the user login activity for PFCS.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

PFCS does not share any information with external organizations.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Not applicable since PFCS does not share any information with external organizations.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Not applicable since PFCS does not share any information with external organizations.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Not applicable since PFCS does not share any information with external organizations.

Section 6.0 Notice

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

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

No.

6.2 Was notice provided to the individual prior to collection of information?

Notice was provided to individuals by the initial source systems prior to collection or processing of the information. PFCS is used internally by authorized RD and FSA staff, so it is not available to the general public, and it is not involved in the initial collection of information from individuals.

6.3 Do individuals have the opportunity and/or right to decline to provide 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. PFCS is used internally by authorized RD and FSA staff, so it is not accessible by the general public, and it is not involved in the initial collection of information from individuals.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Consent of the individuals for uses of the information would have been obtained by the initial source systems, if required, prior to collection or processing of the information. PFCS is used internally by authorized RD and FSA staff, so it is not accessible by the general public, and it is not involved in the initial collection of information from individuals.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Notice was provided to individuals by the initial source systems prior to collection or processing of the information. The initial assessment of privacy risk would be performed by the administrators who manage the data at its collection.

Individuals do not have direct access to the system as users. Notice of the purposes and uses for the collection of the information is provided in the SORN RD-1.

Section 7.0 Access, Redress and Correction

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

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

The public does not have direct access to PFCS; all data is received by USDA personnel from the original source components.

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: Any individual may request information regarding this system of records or determine whether the system contains records pertaining to him/her, from the appropriate System Manager. If the specific location of the record is not known, the individual should address his or her request to: Rural Development, Freedom of information Officer, United States Department of Agriculture, 1400 Independence Avenue SW, Stop 0742, and Washington, DC 20250–0742. A request for information pertaining to an individual must include a name; an address; the RD office where the loan or grant was applied for, approved, and/ or denied; the type of RD program; and the date of the request or approval.

7.2 What are the procedures for correcting inaccurate or erroneous information?

The public does not have direct access to PFCS; all data is received by USDA personnel from the original source components.

Individuals are notified of the procedure to gain access to and contest their information in the Record Access Procedures section as outlined in the SORN RD-1. See Record Access Procedures information in 7.1.

Customers and employees may also contact:

USDA Rural Development Primary FOIA Contact Information:
Lolita Barnes
FOIA Liaison

1400 Independence Ave., SW
Washington, DC 20250
Tel. 202-692-0004
Email: lolita.barnes@usda.gov

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

Individuals are notified of the procedure to gain access to and contest information at the initial point of collection as outlined in the SORN RD-1. See Record Access Procedures information in 7.1.

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

N/A

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

No additional risks are associated with the redress process. The public does not have direct access to PFCS. The requestor may also refer to the RD-1 SORN for additional information regarding Record Access Procedures.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

Desk Procedures document the User Access Management (UAM) Team process for establishing, activating, and modifying individual users for PFCS. The group and account types are defined by the System Owner for PFCS. The Agency's Information System Point of Contact (POC) assigns group membership and determines individual RD user access. The UAM Team creates, modifies and deletes user requests approved by the Agency's Information System Point of Contact.

RD and FSA employees and contractors' access PFCS after being provisioned in eAuthentication by a User Access Management (UAM) ticket, created by the System POC and completed by the UAM Team (UAMT).

Steps to provision RD employees and RD contractors follow desk procedures as set by the system owner for PFCS.

8.2 Will Department contractors have access to the system?

Yes, RD contractors are required to undergo the same access and authentication procedures that RD federal employees follow, as discussed in section 8.1.

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

Yes, all RD employees and contractors are required to complete annual information security and awareness training, which includes privacy training for PFCS.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes, PFCS has an Authorization to Operate (ATO), which is valid until 2/25/2023.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

PFCS complies with the Federal Information Security Modernization Act of 2014 (FISMA) by documenting the Authorization and Accreditation, annual control self-assessments, and continuous monitoring in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev. 4. These controls, including full compliance, inheritance, and risk acceptance descriptions, are available in CSAM. PFCS is hosted on the DISC platform at USDA, which is FedRAMP certified and follows USDA security and privacy requirements.

Access to PFCS is controlled through eAuthentication for authorized PFCS users, and access to sensitive information is controlled through DISC Profiles/Groups on a need-to-know basis with audit logs of user activity for PFCS. Section 5 of this PIA describes security protections in place for PFCS data.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

A privacy risk associated with PFCS could be extracting and using the information erroneously. Since PFCS is used by authorized RD staff using eAuthentication and there are group access management controls, the privacy risks are minimal. Potential compromise of privacy data is mitigated by DISC audit event monitoring and USDA network security protections in place to protect RD data for PFCS on the DISC platform.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

The PFCS "core" is a COTS package using the Oracle Federal Financials, which is Joint Financial Management Improvements Program (JFMIP) certified and meets the basic requirements for Federal Financial Management functions.

For all technologies chosen by RD, an Analysis of Alternatives (AoA) is completed to determine which technologies will be selected and ultimately purchased or built.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No, the project utilizes Agency-approved technologies for PFCS, and these technology choices do not raise privacy concerns. PFCS is hosted on the DISC platform at USDA.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes, the system owner and the Information Systems Security Program Manager (ISSPM) have reviewed the Office of Management and Budget (OMB) memoranda.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Not applicable, PFCS does not use 3rd party websites or applications.

10.3 What personally identifiable information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

Not applicable, PFCS does not use 3rd party websites or applications.

10.4 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

Not applicable, PFCS does not use 3rd party websites or applications.

10.5 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be maintained and secured?

Not applicable, PFCS does not use 3rd party websites or applications.

10.6 Is the PII that becomes available through the agency’s use of 3rd party websites and/or applications purged periodically?

Not applicable, PFCS does not use 3rd party websites or applications.

10.7 Who will have access to PII that becomes available through the agency’s use of 3rd party websites and/or applications?

Not applicable, PFCS does not use 3rd party websites or applications.

10.8 With whom will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be shared - either internally or externally?

Not applicable, PFCS does not use 3rd party websites or applications.

10.9 Will the activities involving the PII that becomes available through the agency’s use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not applicable, PFCS does not use 3rd party websites or applications.

10.10 Does the system use web measurement and customization technology?

No, PFCS does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Not applicable, PFCS does not use web measurement and customization technology.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not applicable, PFCS does not use 3rd party websites or applications.

Approval Signature

Signed copy kept on record.