Privacy Impact Assessment
Program Funds Control System (PFCS)

Policy, E-Government and Fair Information Practices

- Version: 2.0
- Date: February 18, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

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

February 18, 2020

Contact Point

Angela Cole
Rural Development ISSPM
(202)-401-0757

Reviewing Official

Michael S. Gardner
System Owner (SO)
United States Department of Agriculture
(202) 692-0212

Abstract

The Program Fund 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-related funds.

Overview

The Program Fund 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-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. PFCS replaced two existing legacy funds control systems that are mainframe-resident. The new system will provide overall agency fund 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 PFCS "core" is a COTS package using the Oracle Federal Financials, which is 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?

Funds appropriated by Office of Management and Budget (OMB) are entered into PFCS and obligation data is entered from RD and FSA systems. Funds are tracked and each system can obligate funds for their loan and grant programs.

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), Business Intelligence (BI), Commercial Loan Servicing System (CLSS), LoanServ, and Guaranteed Loan System (GLS).

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 fund 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, and GLS 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?

The data is entered into the FSA system, PLAS, BI, CLSS, LoanServ, and GLS systems and passed to PFCS through real time files 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, and GLS) with the amounts in the PFCS system. Balancing is completed against general ledger, allotment summary, and check disbursement. National Finance and Accounting Operations Center (NFAOC) reviews these outputs daily.

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

Information 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*
- *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*
- *RD Records Management Policy*
- *NARA Records Retention*

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 customer.

The PFCS system owner defines access roles to ensure separation of duties, account management and authorized access to data and information in PFCS. Only authorized RD and FSA staff can access the PFCS application using 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, and CLSS systems. Each system can then obligate available funds for program loans and grants. Funds control is required by law to prevent "anti-deficiency", spending more money than is appropriated by Congress. PFCS also sends data to TDW (BI) for 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, CLSS, LoanServ, and GLS) with the amounts in the PFCS system. Balancing is completed against general ledger, allotment summary, and check disbursement. NFAOC reviews these outputs 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 PFCS include DISC audit logs/security logs.

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?

Currently the data is permanently retained and not purged from PFCS.

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 NARA.

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 reports. PFCS has multiple system checkpoints in place that notify the system administrators/operators verifying that all jobs run to completion. Also, the data is stored in a secure environment behind the DISC secure mainframe infrastructure.

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?

BI– Tabular Data Warehouse (TDW) – Sends data for reports

CLSS – Loan Grant Management System (LGMS) sends obligations and advance requests

eServices – Account Cross Reference (ACR) – Request is made to ACR to perform lookup in TDW

GLS– Data is forwarded to MQ series messages to PFCS for specific transactions

LoanServ – Fund distribution/allocation

FSA/PLAS – Accounting system providing transaction processing

4.2 How is the information transmitted or disclosed?

The information within the PFCS applications is transmitted using HTTPS. The information that is shared internally is 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 risk is the unauthorized access and potential compromise of PII data in PFCS.

This privacy risk is mitigated by the DISC Midrange environment, which hosts the PFCS application and provides security and privacy data protection and complies with USDA requirements on protecting information. Also, only authorized RD and FSA staff access PFCS using eAuth, so there are audit logs on this activity.

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?

Department of Treasury, Bureau of the Fiscal Service Treasury Web Application Infrastructure (TWAI) – A tracking system for allocated program funds for PFCS, CLSS, GLS, and LoanServ applications, including Program Loan Accounting System (PLAS) owned by Field Services Agency (FSA). PFCS contains PII information such as name and miscellaneous identification numbers.

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.

Yes, USDA/Rural Development 1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs covers the routine use of this information with the external trusted sources described in section 5.1.

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

Department of Treasury, Bureau of the Fiscal Service TWAI – VPN connection using AES-256 or 3DES encryption. PFCS requires and has in place an Interconnection Service Agreement (ISA) for all external connections.

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

Privacy risks include the potential compromise of PII and sensitive financial information. This is mitigated by the security protections, such as firewalls, DNSSec, encryption of data in transit, and DISC audit logs. Authorized RD and FSA staff access PFCS using eAuth and RD has continuous monitoring from DISC in compliance with FISMA and as required by RD and USDA. PFCS data is stored in a secure environment on the DISC platform.

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.

Yes, it follows Rural Development 1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants and Other Participants in RD Programs, https://www.govinfo.gov/content/pkg/FR-2016-04-28/pdf/2016-09938.pdf.

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

N/A – No data is collected directly from citizens.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

N/A – No data is collected directly from citizens.

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

N/A – No data is collected directly from citizens..

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.

Not applicable. No data is collected directly from citizens.

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?

Not applicable. No data is collected directly from citizens.

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

Not applicable. No data is collected directly from citizens.

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

Not applicable. No data is collected directly from citizens.

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

Not applicable. No data is collected directly from citizens.

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

Not applicable. No data is collected directly from citizens.

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 applications. The 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 System Point of Contact.

RD employees and RD contractors access PFCS after being provisioned by a User Access Management (UAM) ticket, created by the System POC and completed by the UAM Team (UAMT). Access is granted via eAuth.

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 ATO, which is in CSAM.

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. PFCS is hosted on the DISC Midrange environment at USDA, which are FedRAMP certified and follow USDA security and privacy requirements.

Access to PFCS is granted via eAuth once the UAM completes the proper provisioning. 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?

Since PFCS is used by authorized RD and FSA staff using eAuth 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 in the DISC Midrange environment.

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 all 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.

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 ISSPM have reviewed the OMB memorandums.

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?

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

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 3rd party websites or applications.

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.

Responsible Officials

ANGELA COLE
Digitally signed by ANGELA COLE
Date: 2020.02.20 15:57:57 -05'00'

Angela Cole
Information Systems Security Program Manager (ISSPM)
Rural Development
United States Department of Agriculture

Approval Signature

MICHAEL GARDNER
Digitally signed by MICHAEL GARDNER
Date: 2020.02.21 09:29:59 -05'00'

Michael S. Gardner
System Owner
Rural Development
United States Department of Agriculture