Privacy Impact Assessment

Program Funds Control System (PFCS)

Rural Development (RD)

- Date: August 24, 2017
- Prepared for: RD

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	9/8/2014	SAC	Original under CLP
1.1	7/11/2016	TGW	FY 16 review
1.2	4/27/2017	TGW	Updating internal/external connections (sections 4 and 5)
1.3	8/24/2017	TGW	FY18 annual review

Abstract

PFCS replaced the appropriation accounting systems and automated manual processes which were integrated into four large, legacy systems. PFCS is independent from these systems, but supports all budget, funds management, funds control, and funds reporting functions required by those loan and grant program legacy systems. PFCS provides financial data in electronic form for posting to the existing Financial General Ledger system.

Overview

PFCS access originates from a personal computer (PC) or laptop computer at Farm Services Agency (FSA) and RD finance offices, FSA and RD budget offices including FSA and RD program management offices. Agencies' offices obtain access to the application on the NITC Midrange through established channels. Each user is required to request access authority and, upon approval, is provided an Identification (ID) allowing only appropriate access. Additionally, no major changes have been required to the NITC Midrange to support PFCS.

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?

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?

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.).

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

RISK: The privacy risks identified are based from funds appropriated by Office of Management and Budget (OMB) and 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. The risk is in the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the client.

MITIGATION: Data is stored in a secure environment behind the NITC secure mainframe infrastructure. See the System Security Plan (SSP) security controls Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM).

.

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.

No data is collected from commercial or public sources.

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 National Institute of Standards and Technology (NIST) 800-53 controls for the CLP Servicing - PFCS are discussed in detail in the System Security Plan and specifically the Access Controls (AC-1-8, 12, 14, 17), Identification and Authentication (IA- 1-7) controls are in place to prevent unauthorized access restricting users from accessing the operating system, other applications or other system resources not needed in the performance of their duties and is restricted by Active Directory (AD) User Identification (User ID). Authority and Purpose (AP) compensating control gives explanation of why PII is allowed on the system. Systems and Communication Protection (SC-1, 2, 4, 5, 7, 8, 10, 12, 13, 17, 20-23, 28, and 39) controls are in place to prevent unauthorized access.

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

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

RISK: Currently the data is permanently retained and not purged from PFCS although minimal risk associated with funds tracking. With data stored for this length of time there is always the potential of unauthorized access, unauthorized disclosure or illegal use of the customer PII data.

MITIGATION: 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 NITC secure mainframe infrastructure. See the System Security Plan (SSP) security controls Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM).

.

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?

FSA and RD Budget Staffs initially enter approved funding data into PFCS. Apportionments, allocations, and distributions are subsequently established by Budget, Financial, and Program management staffs based on legislative and regulatory directives and guidance. Funds requests, in the form of transactions such as reservations, commitments, and obligations (all of which can originate at service center, district, state or national office levels), are then processed verifying funds availability for that specific action. If funds are available, the request is approved and updates the files accordingly, reducing the amount of funds available for the next request. Reports, ad hoc as well as fixed format, are available through online query and/or overnight

processing. Funding information is available to all management levels upon request, and is more timely and accurate than in the previous environment.

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.

RISK: The risk to internal information sharing would be the unauthorized disclosure of application obligations and advance requests, specific transaction data, and fund distribution and allocations.

MITIGATION: The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality. The security and control of PII is the responsibility of the System Owner and RD employees. Risk is mitigated with the implementation of RD ISSS NIST policies, standards and procedures. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure.

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.

PFCS is covered under, USDA/Rural Development-1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs.

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.

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

RISK: The risk to external information sharing would be the unauthorized disclosure of application obligations and advance requests, specific transaction data, and fund distribution and allocations.

MITIGATION: Data is sent via VPN connection using AES-256 or 3DES encryption, and signed Interconnection Service Agreement are in place in CSAM and maintained by the ISSS. The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality. The security and control of PII is the responsibility of the System Owner and RD employees. Risk is mitigated with the implementation of RD ISSS NIST policies, standards and procedures. Also, the data is stored in a secure environment behind the NITC secure mainframe infrastructure.

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, USDA/Rural Development-1 Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants, and Other Participants in RD Programs (http://www.ocio.usda.gov/policy-directives-records-forms/records-management/system-records)

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.

N/A – 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?

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

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

N/A – No data is collected directly from customers and employees.

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

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

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

N/A – 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.

N/A –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?

Generally, the National Institute of Standards and Technology (NIST) 800-53 controls are discussed in detail in the System Security Plan (SSP) and specifically the Access Control (AC), Identification and Authentication (IA) and Systems and Communication Protection (SC) controls are in place to prevent unauthorized access. Access control is also addressed in the individual systems desk procedures.

Desk Procedures document the process for establishing, activating, and modifying IDs. This process is defined by System Owners. System Owners define Groups and account types. System Point of Contact assigns group membership and determines Need-to-know validation. The POC is responsible for verifying user identification; the User Access Management (UAM) Team relies on a POC supplying the correct UserID and password. UAM tickets are the tool used to track authorized requests by approving POC.

RD reviews reports from HR on a Bi-weekly basis. The organization employs automated mechanisms to support the management of information system accounts. Temporary and emergency accounts are not used or authorized. Guest and Anonymous accounts are not managed by ISS UAM Team. POCs (empowered by RD IT managers) are responsible for notifying UAM Team if access or roles need to be modified and periodically reviewing and certifying established access.

Access is controlled by UserID and password. Access rights are granted to designated individuals only when a written request is approved by their supervisor. The User Access Management (UAM) Team follows procedures to provide access to the system. The ISSS personnel approve and process elevated access request. The procedures are documented.

8.2 Will Department contractors have access to the system?

Yes, access is granted upon approval by a supervisor, Information Systems Security Staff (ISSS), Point of Contact (POC) and ISSS Security User Access Management (UAM) Team staff.

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

USDA RD requires annual Information Security and Awareness Training (ISAT) for all employees and contractors. RD is responsible for ensuring all new employees and contractors

have taken the Department Security Awareness Training developed by Office of Chief Information Officer-Cyber Security. Training must be completed with a passing score prior to access to a USDA RD system. All RD employees/contractors are required to complete Computer Security Awareness Training on an annual basis.

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

Yes

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

NIST 800-53 controls are discussed in detail in the SSP including the Audit and Accountability (AU) controls in place to prevent misuse of data.

RD has a NIST Audit and Accountability Policy, Standards, and Procedure that defines the following auditable events: server startup and shutdown, loading and unloading of services, installation and removal of software, system alerts and error messages, user logon and logoff attempts (both successful and unsuccessful), granting of elevated privileges (root access success and failure), modifications of privileges and access controls, all root commands (success and failure), and sensitive files accessed, modified and added. These controls, including full compliance, inheritance, and risk acceptance descriptions, are available in CSAM.

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?

RISK: There is minimal risk given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system,.

MITIGATION: However, RD has the following controls in place - collecting auditable events: date and time of the event, the component of the information system where the event occurred, type of event, user/subject identity, and the outcome (success or failure) of the event. Audit logs will be reviewed by the NITC Security Division every two weeks and suspicious activity will be investigated. Suspicious activity includes, but not limited to: modifications or granting of privileges and access controls without proper request submitted, consecutive unsuccessful log-on attempts that result in a user being locked, multiple unsuccessful log-on attempts without lock out by the same User Identification (UserID), modifications or attempted modification of sensitive files without authorization and within the applications repeated attempts to access data outside a user's privilege.

Per the General Records Schedule 20 Section 1C, the following items will be deleted/ destroyed when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes: electronic files and hard copy printouts created to monitor system usage,

including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system usage.

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.

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

No, PFCS does not employ technologies which would 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 guidance was reviewed, however, the system does not use 3rd party websites and/or applications.

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

PFCS does not use 3rd party websites and/or applications.

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

PFCS does not use 3rd party websites and/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?

PFCS does not use 3rd party websites and/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?

PFCS does not use 3rd party websites and/or applications.

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

PFCS does not use 3rd party websites and/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?

PFCS does not use 3rd party websites and/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?

PFCS does not use 3rd party websites and/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)?

PFCS does not use 3rd party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

PFCS does not use 3rd party websites and/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?

PFCS does not use 3rd party websites and/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.

PFCS does not use 3rd party websites and/or applications.

Responsible Official

JANET HAVELKA Digitally signed by JANET HAVELKA
Date: 2017.10.17 08:42:28 -05'00'

Janet Havelka
Chief, Mortgage Loan Technologies Branch

Approval Signature

EUGENE TEXTER Digitally signed by EUGENE TEXTER
Date: 2017.10.17 12:16:53 -05'00'

Diego Maldonado
Rural Development Privacy Officer