5.

Privacy Impact Assessment
LoanServ

Rural Development (RD)

- Date: August 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	7/13/2016	TGW	FY 16 review
1.1	2/7/2017	TGW	FY17 review, no changes
1.1	8/25/2017	SAC	FY18 review, no changes

Abstract

LoanServ is used to provide loan servicing and support for all rural housing direct loans and grants, including delinquency servicing and risk management. It also provides the interfaces to taxing authorities, insurance providers, credit bureaus, the U.S. Department of Treasury for the Treasury Offset Program and Cross Servicing for Guaranteed Loss Claims, and other entities.

DLATS EDIs purpose is to enable the Customer Servicing Center (CSC) to receive bankruptcy notices electronically.

CallPeg is a software application designed to provide CSC with a tool to capture reasons customers call in to the Call Center.

Overview

The LoanServ system is used to provide loan servicing and support for all rural housing direct loans and grants, including delinquency servicing and risk management. The LoanServ system also provides the interfaces to taxing authorities, insurance providers, credit bureaus, the U.S. Department of Treasury for the Treasury Offset Program and Cross Servicing for Guaranteed Loss Claims, and other entities which assist in providing a secure and robust loan servicing system. Both DLATS EDI and CallPeg are modules under LoanServ.

- DLATS EDI

  DLATS EDI enables the CSC to receive bankruptcy notices electronically. The DLATS mailbox pushes the electronic bankruptcy notices to the secure file transfer protocol (SFTP) server in the X-12 format. The notices are created by a flat file and then sent via SFTP to a CSC server.

- CallPeg

  CallPeg is a software application designed to provide CSC with a tool to capture reasons customers call in to the Call Center. Some of the data captured include account number, reason(s) for call, representative answering the phone and date and time along with some current account data such as customer delinquency. RD then uses this information to study the call activity and to improve the quality of customer service they provide.

NOTE: *Per the PTA, DLATS EDI does not require a PIA and will not be included in the remainder of the document.*

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?

LoanServ: Borrower and co-borrower names, social security numbers, phone numbers, addresses, financial data, repayment information, and tax and hazard insurance information.

CallPeg: The customer's name (full name, mother's maiden name, maiden name of the individual, nickname or alias). Miscellaneous identification numbers (agency assigned number, case number, accounts or permits).

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

LoanServ receives closing documentation, phone and personal interviews, and correspondence via UniFi (loan origination system). The cross reference feature in FiServ, Loan Servicing platform allows users to search on any of the listed criteria for the particular borrower record, as well as Flood Tracking Number where applicable.

CallPeg receives the information from LoanServ application.

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

LoanServ information is collected, used, disseminated or maintained for the servicing of the loans, the payment of taxes and insurance bills on the property and the reporting of payment history to the credit bureaus.

CallPeg information is used to collect reasons for calls to the call center giving management business intelligence on calls allowing them to better manage call center.

1.4 How is the information collected?

LoanServ: The information is collected via upload from UniFi (loan origination system), closing documentation, phone and personal interviews, and correspondence.

CallPeg: When users finish a call, the analyst records the call reason by choosing one or more options from a dropdown list along with who called "Peg the Call". At that time they can also enter notes that are sent to the noting system in LoanServ via an application to application API call.

1.5 How will the information be checked for accuracy?

LoanServ, CallPeg: Application software contains internal edits to ensure data integrity.

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: With LoanServ the risk is to borrower and co-borrower names, social security numbers, phone numbers, addresses, financial data, repayment information, and tax and hazard insurance information. With CallPeg the risk is to the customer's name (full name, mother's maiden name, maiden name of the individual, nickname or alias), miscellaneous identification numbers (agency assigned number, case number, accounts or permits). 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.

Data is used in all aspects of loan servicing of Single Family Housing (SFH) direct loans and grants. Servicing includes payment application, delinquency processing, automated escrow accounts and default management identify call reason trends, and type of calls to the center.

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

Application software contains internal edits to ensure data integrity.

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

LoanServ: Tax Identification Numbers (Parcel Number) are available to the public and must be used in order to pay the borrowers real estate tax bills and is a matter of public record. Addresses are verified determining accuracy of mailing addresses. Bankruptcy and Foreclosure data is collected to ensure no violation of bankruptcy and foreclosure laws occurs.

CallPeg: N/A

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 LoanServ application is discussed in detail in the System Security Plan and specifically the Access Controls (AC 1-8, 11, 12, 14, 17, 20, and 21), Identification and Authentication (IA 1- 8) and Systems and Communication Protection (SC 1, 2, 4, 5, 7-10, 14, 17, 20-23, 28, and 39) controls are in place to prevent unauthorized access.

NIST SP 800-53 security controls for the **LoanServ** and **CallPeg** applications are discussed in detail in the Security Control Compliance Descriptions within Cyber Security Assessment Management (CSAM).

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?

LoanServ: Loan origination information is kept on the system for the life of the loan. Tape backups of all data are stored for 15 years.

Call Peg: A reporting tool where reports are kept indefinitely logging who took the call, subject and who received the call.

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: LoanServ: Loan origination information is kept on the system for the life of the loan. Tape backups of all data are stored for 15 years. Call Peg: A reporting tool where reports are kept indefinitely logging who took the call, subject and who received the call.

MITIGATION: Once data is no longer needed, it is properly destroyed. Methods such as overwriting the entire media, degausses, and disk formatting are used, but strict attention is paid to whatever process is selected to ensure that all unneeded data is completely destroyed. Papers and other soft materials, such as microfiche and CD's, are shredded. 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?

LoanServ:

- New Loan Originations – UniFi data is used to update application information in the LoanServ loan servicing application
- Automated Mail Processing (AMP) – Print service for statements and tax forms
- Business Intelligence (BI) – FOCUS and Tabular Data Warehouse (TDW) – Provide data for reports to both LoanServ and DLATS EDI
- Program Funds Control System (PFCS) – Loan funds distribution
- Common Call Component – ECF/Imaging – Provides LoanServ loan information storage/retrieval
- eServices – NowChecks - NowChecks retrieves Escrow disbursement files are created in the LoanServ application
- CLP Support Admin – MortgageLink - Provided links to LoanServ CICS region.
- Program Loan Accounting System (PLAS) – Accounting system providing transaction processing

CallPeg: The system receives the account number and customer name from LoanServ; therefore, the call can be tied to the customer who called.

4.2 How is the information transmitted or disclosed?

Internal data information is transmitted via scheduled job.

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 information, statements and tax forms or loan information storage/retrieval.

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?

LoanServ

- CBC Innovis Credit Bureau – LoanServ provides monthly credit bureau information to disseminate in compliance with the Fair Credit Reporting Act (FCRA)
- Corelogic Web Portal - Provides capability for the real estate taxing authorities to process billing information for several mortgage companies in a single file.
- FiServ – Hazard EDI - Data files received from the designated hazard insurance carriers are automatically routed to a proprietary third-party EDI translation application that converts each file back to LoanServ hazard insurance format.
- Experian Credit Bureau - LoanServ provides monthly file FCRA transmitted to Experian for collection and disseminate as required. Data files transferred from LoanServ, CLSS and GLS to Experian for credit bureau reporting.
- Express Payment Money Gram - Allows customers to make urgent payments or pay routine bills through MoneyGram's network to certain creditors.

- Fiscal Service Treasury Web Application Infrastructure (TWAI) Department of Treasury - U. S. Department of Treasury provides debtor and debt information for Treasury Offset Program and Cross Servicing processing
- Global Exchange Services – DLA Tran-Serv GEX – DLA Transaction Services GEX provides a daily file containing federal bankruptcy X12 data to USDA.
- Veterans Administration - Processing and oversight of USDA's Real Estate Owned (REO) Properties.
- Proctor EDI - Provide force-placed hazard insurance to borrowers.
- SunTrust - Escrow disbursement account information is transmitted to SunTrust via Online File Transfer.
- TransUnion Credit Bureau - LoanServ provides monthly file FCRA transmitted to Experian for collection and disseminate as required.
- US Bank - U.S. Bank provides lockbox services for the Application's direct single family housing loan customers.
- Western Union - Western Union's Walk-in Cash Payments allows consumers to make urgent payments or pay routine bills through their network to certain creditors.

CallPeg: N/A

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.

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

CallPeg: N/A

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

LoanServ: All external connections require an Interconnection Service Agreement (ISA) or Memorandum of Understanding (MOU).

- CBC Innovis Credit Bureau – CBCInnovis returns a credit report via an Internet API call to the securecreditbureaureports.com web portal over HTTPS with files being transferred over Connect Direct using SSL for encryption.

- Corelogic Web Portal – All data files transmitted are sent using Commerce's Connect Direct over IP with Security+ for encryption.
- FiServ – Hazard EDI – FiServ uses PGP encryption to dedicated FTP Servers for State Farm Insurance, Farmers Insurance and Travelers Insurance. FiServ also provides DMZ server using a password secured connection to Allstate Insurance, American Family Insurance and Nationwide Insurance.
- Experian Credit Bureau - LoanServ provides monthly file FiServ Credit Bureau Reporting to Experian are transferred over the internet using HTTPS via SSL.
- Express Payment Money Gram – MoneyGram creates a payment posting file and puts it on their FTP server (encrypted and zipped). All data files sent to NITC mainframe use PKWARE and AES 256 encryption. USDA logs into the MoneyGram server using UserID and password, decrypts it and puts it on the NITC mainframe. A UserID and password is needed to retrieve this file. After USDA retrieves this file, MoneyGram deletes it from their mailbox.
- Fiscal Service Treasury Web Application Infrastructure (TWAI) Department of Treasury - U. S. Department of Treasury - Connect:Direct without Secure+ uses a proprietary file transfer protocol (TCP ports 1364 and 1372).
- Global Exchange Services – DLA Tran-Serv GEX – DLA Transaction Services GEX provides a daily file containing federal bankruptcy X12 data to USDA using SFTP to a Linux server.
- Veterans Administration – data to be transferred bi-directional consisting of account identification (ID) and property, account, sale and expense information.
- Proctor EDI – Mainframe to mainframe file transfer over VPN.
- SunTrust - Escrow disbursement account information is transmitted to SunTrust via Online File Transfer via HTTPS.
- TransUnion Credit Bureau – All information transferred from LoanServ to TransUnion is sent using SSL, is one-directional with RD individual logon to the TransUnion FTP server. No direct connection between LoanServ and TransUnion is established.
- US Bank – STOP files are transferred over the internet via HTTPS and secure socket layer for encryption
- Western Union – creates a zip file uploading to their SFTP server, USDA retrieves this file via specific IP address with unique UserID and password. Once the file is retrieved, USDA deletes the file from the mainframe. Western Union retains the file on their server for 14 days after which it is automatically deleted.

CallPeg – N/A

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 statement and tax report information, borrower information and accounting information.

MITIGATION: Data is sent via an Internet API call to the securecreditbureaureports.com web portal over HTTPS with files being transferred over Connect Direct using SSL for encryption, and signed Interconnection Service Agreements 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.

CallPeg – N/A

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

https://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?

LoanServ: Yes, at the time of loan application, Form RD410-4 contains the privacy act notice.

CallPeg: N/A

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

LoanServ: Yes.

CallPeg: N/A

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

LoanServ: No, RD410-4 indicates all possible uses of the information.

CallPeg: N/A

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.

LoanServ: RD410-4 is provided at the time of loan/grant application. If an individual does not sign the application, it will result in the rejection of the loan/grant application. Applicants are not unaware of the collection of personal information.

CallPeg: N/A

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?

LoanServ: Individuals are provided a customer service telephone number (800-414-1226) to verify information on their account. .

CallPeg: N/A

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

LoanServ: Individuals should be instructed to call customer service (800-414-1226) to have changes made regarding incorrect information

CallPeg: Information can be corrected when the customer calls.

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

LoanServ: Field Office personnel will give the borrower the customer service number to call. The monthly billing statement also provides procedures for correcting their information.

CallPeg: N/A

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

LoanServ: Formal redress is provided, via reconsideration, mediation, and arbitration.

CallPeg: 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.

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?

National Institute of Standards and Technology (NIST) 800-53 controls for LoanServ are discussed in detail in the System Security Plan 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 Team (UAMT) relies on a POC supplying the correct UserID and password to UAM to identify themselves. UAM tickets are the tool used to track authorized requests by approving Point of Contact (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 UAMT if access or roles need to be modified and periodically reviewing and certifying established access.

8.2 Will Department contractors have access to the system?

Yes, Department contractors are required to undergo the same access and authentication procedures that federal employees must adhere to, access procedures are discussed in question 8.1.

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 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 OCIO-CS. Training must be completed with a passing score prior to access to a USDA RD system.

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

Yes, the current ATO is valid until 28 February 2020.

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

RD has an Application Auditing and Monitoring Policy in place 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 Cyber Security Assessment and Management (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?

LoanServ is a COTS product which has been significantly enhanced to accommodate the unique requirements of the Housing loan programs.

CallPeg software application is designed to provide CSC with a tool to capture reasons customers contact the Call Center.

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

No.

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?

LoanServ applications do not use third 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.

LoanServ applications do not use third 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?

LoanServ applications do not use third 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?

LoanServ applications do not use third 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?

LoanServ applications do not use third 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?

LoanServ applications do not use third 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?

LoanServ applications do not use third 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)?

LoanServ applications do not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

LoanServ 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?

LoanServ 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.

LoanServ applications do not use third party websites or applications

Responsible Officials

JANET HAVELKA Digitally signed by JANET HAVELKA
Date: 2017.10.11 10:13:46 -05'00'

Janet Havelka
Chief, Mortgage Loan Technologies Branch

Approval Signature

EUGENE TEXTER Digitally signed by EUGENE TEXTER
Date: 2017.10.13 13:53:19 -05'00'

Diego Maldonado
Rural Development Privacy Officer