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

USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	LoanServ
Program Office	Technology Office | Information Assurance
Mission Area	Rural Development
CSAM Number	2113
Date Submitted for Review	09/23/2025

Mission Area System/Program Contacts

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

Abstract

LoanServ is used to provide loan servicing and support for rural housing SFH (Single Family Home) direct loans and grants, including delinquency servicing and risk management. LoanServ 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 for required financial reporting. This PIA is required because the PTA determined that PII data is processed in LoanServ.

Overview

The LoanServ loan servicing system is a Commercial-off-the- Shelf (COTS) product which has been significantly enhanced to accommodate the unique requirements of the Federal Housing loan programs. The purpose of LoanServ is to provide loan servicing and support for single family housing direct loans and grants (payment application, delinquency processing, automated escrow account processing and required financial reporting to credit bureaus and Treasury). 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 other entities which assist in providing a secure and robust loan servicing system.

Primary users of LoanServ work in the Servicing Office (SO), Office of the Deputy Chief Finance Officer, State and Local servicing offices, and the National Office. PII is processed.

Call Pegging (CallPeg) is a software application tool within the LoanServ area boundary used by USDA Servicing Office (SO) designed to capture reasons customers call in to the Call Center. The CallPeg system piggybacks on the LoanServ application. Information collected includes the account number, reason(s) for call, representative's name answering the call, date and time, and some current account data such as customer delinquency. RD uses this information to study the call activity and to improve the quality of customer service they provide. PII is processed.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

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

- Consolidated Farm and Rural Development Act (7 U.S.C. §1981, 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, Section 6417)
- Fair Credit Reporting Act, 15 U.S.C. §1681f
- Consumer Credit Protection Act, 15 U.S.C. §1601, et. seq.
- Equal Credit Opportunity Act, 15 U.S.C. §1691, et. seq.
- The Fair Debt Collection Practices Act, 15 U.S.C. §162, et. seq.
- 7 CFR Part 3550, Direct Single Family Housing Loans and Grants
- 7 CFR Part 3555, Guaranteed Rural Housing Program
- 7 CFR Part 3560, Direct Multi-Family Housing Loans and Grants

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

Yes, ATO expires 01/02/2026

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

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

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

No

Section 2: Characterization of the Information

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

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

Identifying Numbers:

- Social security numbers
- File/Case ID number

Biographical Information:

- Name (including nicknames)
- Ethnicity
- Home address
- Personal email address
- Employment information
- Date of birth (MM/DD/YY)

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

LoanServ receives closing documentation for Single-Family Housing (SFH direct loans and grants, phone and personal interviews, and correspondence from UniFi (an internal RD application), which is the loan origination system.

CallPeg gets its information from customer calls and is tracked internally and hosted on the DISC platform. SO representatives capture reasons customers call in to the Call Center. with.

How is the information collected?

LoanServ information is collected from UniFi with an upload that contains closing documentation for the SFH direct loans and grants, phone and personal interviews, and RD correspondence.

CallPeg information is collected from RD customers who call RD staff for assistance.

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

No

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

The data is verified by authorized RD staff with regular review and verification as part of the normal workflow for LoanServ. Authorized RD Staff routinely review the information to ensure its accuracy as part of the normal workflow for LoanServ.

Does the system/program use third-party websites?

No

What is the purpose of the use of third-party websites?

N/A

What PII will be made available to the agency though the use of third-party websites?

N/A

Privacy Impact Analysis: Related to characterization of the information.

Privacy Risk

- **Misclassification of Data**: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.
- **Inadequate Security Controls**: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.
- **Over-collection of Data**: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation

- **Data Classification Policy**: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.
- **Regular Data Inventory**: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.
- **Contextual Information Use**: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.
- Risk is also mitigated with internal security and privacy controls outline in the System Security Plan. Access is limited to authorized personnel using E-Authentication. Audit logs are maintained to monitor activity. System Owners define access roles to ensure separation of duties, privileged access, and the concept of least privilege. Access to a system is requested and authorized via UAM. All users must have an eAuth Level 2 account to access Loanserv.

Section 3: Uses of the Information

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

Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

LoanServ information is used to process Single Family Housing (SFH) direct loans and grants. This process includes payment application, delinquency processing, automated escrow account processing and required financial reporting to credit bureaus and Treasury.

CallPeg used data for trend analysis to improve the customer relationship for calls made to the call center. RD uses this information to study the call activity and to improve the RD customer experience with enhanced business processes.

Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

LoanServ creates output files that are loaded to the TDW for portfolio reporting. RD uses CallPeg as a reporting tool to study the call activity and to improve the quality of customer service they provide.

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk

- **Unauthorized Use of Data**: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.
- **Data Misuse**: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.
- **Inadequate Consent**: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Mitigation:

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

- **Regular Training**: Provide regular training for employees on privacy laws and the importance of adhering to the defined uses of personal information to ensure compliance.

Section 4: Notice

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

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

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

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

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

Privacy Impact Analysis: Related to notice.

Privacy Risk

- **Inadequate Disclosure**: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.
- **Ambiguity**: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.
- **Non-compliance with Regulations**: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

Mitigation

- **Clear Communication**: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.
- **Regular Updates**: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.
- **User Consent**: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Section 5: Data Retention

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

What information is retained and for how long?

- Loan Serv - RD GRS 2033a SFH Exhibit O
- LOANS: 7 years after Cutoff
- Approved:
  - Line 6 – Sec 502 (Direct Single Family Housing Loans) DAA-0572-2017-0001-0006
  - Line 8 – Sec 502 (Self-Help Housing Loans), DAA-0572-2017-0001-0008
  - Line 7 – Sec 504 (Direct Rehabilitation Loans) DAA-0572-2017-0001-0007
- Rejected, withdrawn, canceled, or expired: Line 4, DAA-0572-2017-0001-0004
- Call Peg – SFH Correspondence 7 FYs after Cutoff, DAA-0572-2017-0001-0001

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Yes

Privacy Impact Analysis: Related to retention of information.

Privacy Risk

- **Excessive Data Retention**: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.
- **Data Breaches**: The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.
- **Non-compliance with Regulations**: Failing to adhere to legal requirements regarding data retention periods can lead to regulatory penalties and legal liabilities.
- **Obsolescence of Data**: Retained data may become outdated or irrelevant, leading to inaccuracies in decision-making or service delivery, which can affect individuals negatively.

Mitigation

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

Section 6: Information Sharing

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

With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

LoanServ shares cash tracking, general ledger, and borrower files (name, SSNs) with USDA Farm Production and Conservation (FPAC) for the purpose of reducing operating costs, improving functionality and efficiency, and centralizing access to data.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk

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

Mitigation

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

With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

External Sharing Entity	Types of Data	Purpose
Bank of America	• Full name • Borrower account number • Bank of America account number	Disburse service for escrow account balances
CoreLogic	• Name • Loan number • Address • Tax ID	Provide real estate taxing authorities with tool to process billing information for several mortgage companies in a single file (real estate tax processing)
Dawson's Realty & Mortgage, Inc. Equator	• Names • Addresses • SSN • Financial Data • Loan Number	Provides Loan Data related to Foreclosures and REO accounts and corresponding documents from ECF
DLA & Global Exchange Services (GEX)	• Names • Addresses • SSN • Bankruptcy information	Daily federal bankruptcy data
Experian	• Name • Address • Loan # • SSN	Compliance with Fair Credit Reporting Act (FCRA) (credit reporting)
FiServ Hazard EDI	• Name • Loan # • Address • Policy number	Hazard insurance payment processing
Innovis Data Solutions	• Name • Address • Loan # • SSN	Compliance with Fair Credit Reporting Act (FCRA) (credit reporting)
Information Systems & Networks Corp (ISN) Insight	• Name • Address • Loan # • SSN • Financial Data	Provides Loan Data related to Foreclosures and REO accounts and corresponding documents from ECF
MoneyGram	Loan number	Processing payments

External Sharing Entity	Types of Data	Purpose
Proctor EDI	• Name • Loan # • Address • Policy number	Provide force-place insurance to borrowers
TransUnion	• Name • Address • Loan # • SSN	Compliance with Fair Credit Reporting Act (FCRA) (credit reporting)
US Bank	Loan number	Provides lockbox services for direct single family housing loan customers
US Treasury (TWAI)	• Name • Data/Place of birth • Address • Personal ID number • Financial data • Employment history • Miscellaneous ID numbers	Compliance with Treasury Offset Program and Cross Servicing for Guaranteed Loss Claims
Western Union	Loan number	Processing payments

LoanServ requires an Interconnection Service Agreement (ISA) or Memorandum of Understanding (MOU) for all external connections. The table below describes how data is transferred and the security measures in place:

External Sharing Entity	Transfer method / security measures
Bank of America	Online File transfer via SSL / encryption
CoreLogic	VLAN / encryption
Dawson's Equator DLATS EDI Bankruptcy	• SSL, SFTP / encryption • Electronic Data Interchange (EDI) Secure File Transfer Protocol (SFTP) / encryption
DLA & GEX	VLAN / SFTP transmissions
Experian	SSL, SFTP / encryption
FiServ Hazard EDI	VLAN / encryption
Innovis Data Solutions ISN Insight	• VLAN / 256-bit encryption • SSL, SFTP / encryption
MoneyGram	VLAN / encryption
Proctor EDI	VLAN / Secure FTP over port 990
TransUnion	VLAN / SSL

External Sharing Entity	Transfer method / security measures
US Bank	VLAN / SSL encrypts the data from server to server
US Treasury (TWAI)	Connect:Direct over the TWAI File Transfer Gateway (FTG) and VLAN / Encryption
Western Union	VLAN / via an SFTP server

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk

Moderate Risk: Privacy risks include the potential compromise and unauthorized access of PII data.

Mitigation

This risk is mitigated with internal security and privacy controls outline in the System Security Plan and the ISAs. These measures enforce user authentication and authorization. The system is designed to confirm the identity of authorized LoanServ users prior to granting the appropriate system access based on the user's pre-defined access level. Audit logs are maintained to monitor activity.

Section 7: Redress

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

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

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

What are the procedures for correcting inaccurate or erroneous information?

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

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

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

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

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

Privacy Impact Analysis: Related to redress.

Privacy Risk

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

Mitigation

Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

Section 8: Auditing and Accountability

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

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

Desk Procedures document the process for establishing, activating, and modifying individual users for LoanServ. The group and account types are defined by the System Owner for LoanServ.

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

Desk Procedures document the process for establishing, activating, and modifying individual users for LoanServ. The group and account types are defined by the System Owner for LoanServ.

How does the program review and approve information sharing requirements?

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

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

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