



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	4
Mission Area System/Program Contacts	4
Abstract	5
Overview	6
Section 1: Authorities and Other Requirements.....	7
Section 2: Characterization of the Information.....	8
Section 3: Uses of the Information	10
Section 4: Notice	11
Section 5: Data Retention	12
Section 6: Information Sharing.....	13
Section 7: Redress.....	15
Section 8: Auditing and Accountability	16

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	RD Mainframe Hosted Applications (RD MHA)
Program Office	N/A
Mission Area	USDA - RD
CSAM Number	2653
Date Submitted for Review	01/06/2026

Mission Area System/Program Contacts

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

Abstract

Rural Development (RD), Technology Office Cyber Security Division (CSD) has the RD Mainframe Hosted System. It comprises of the following applications: Automated Mail Processing (AMP), and FOCUS.

Overview

Automated Mail Processing (AMP)

The purpose of AMP is to provide financial enterprise print and mail-handling services to RD, the Farm Production and Conservation (FPAC), National Resource Conservation Service (NRCS), Agricultural Marketing Service (AMS), Federal Grain Inspection Service (FGIS) and other on-demand Federal agencies. AMP produces and distributes financial and management reports, as well as loan servicing and customer notification correspondence for all program areas. AMP produces and distributes financial and management reports, as well as loan servicing and customer notification correspondence as outlined in the above paragraph.

The volume of printed material exceeds 16 million pieces of mail per year and supports an average of 475,000 pieces of metered mail per month. AMP consists of three components: Mail Preparation, Printing, and Mail Insertion.

Mail Preparation System

The mail preparation process uses mail processing software: for address data entry, correction, deliverability, standardization, zip code correction and additions; to certify the accuracy of mail and maximize postal discounts for all classes of mail; and to create presort mailings, and separate mail, among other functions. Additionally, this software creates a print stream and the Mail Run Data File (MRDF). MRDF is a machine-readable barcode used by the insertion system for mail insertion, processing, and control purposes only. The software processes borrower PII data from financial systems of record to create hard copy loan servicing documents and Internal Revenue Service (IRS) tax forms.

Printing System

The printing system consists of a print server, high-speed laser printers, a print queue manager. The print engine prints the jobs produced by the Mail Preparation System. The application processes PII created from the mail preparation system.

FOCUS

FOCUS is a business intelligence tool that produces reports from data residing on the Mainframe and other applications (AMAS, GLS, LoanServ/DLOS, PLAS). FOCUS is not accessible by the public. The purpose of FOCUS is to provide a complete information control system with comprehensive features for entering, maintaining, retrieving, and analyzing data. RD mainly utilizes the end-user reporting features of the FOCUS software. FOCUS processes PII.

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. §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 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, approved 7/30/2025 and expires 8/15/2026.

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

RD-1 SORN, 89 FR 72820, September 6, 2024.

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

N/A

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 number
- File/Case ID number
- Truncated or partial social security number

Biographical Information:

- Name (including nicknames)
- Home address
- Personal Financial Information (Including loan information)

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

- AMP Mail Preparation:
- Automated Multi-Family Account System (AMAS)
- Guaranteed Loan System (GLS)
- LoanServMulti-Family Integrated System (MFIS)
- FOCUS (receives):
- Program Loan Accounting System (PLAS)
- Automated Multi-Family Account System (AMAS)
- Guaranteed Loan System (GLS)
- LoanServ/DLOS

How is the information collected?

- AMP - Information is collected from the financial accounting systems listed under Section 2.2 above.
- FOCUS - All data is derived from other internal systems listed under Section 2.2 above.

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?

N/A

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

MODERATE RISK- Given the amount/type of PII collected this system is classified as a medium privacy risk. AMP processes PII information from internal applications located in a secure network environment within USDA. Current risks are the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the borrower, if an individual, and on the tenant.

Mitigation

Any PII information is automatically deleted within 60 days of the creation of the print job. The information printed contains PII and appropriate administrative, physical, and technical privacy controls are being applied. The AMP equipment is secured by a multi-level, defense-in-depth approach. The equipment is housed in a specifically controlled room in a secure facility with physical access controls at both the facility and room levels. Network connectivity is secured with VLAN isolation of the AMP equipment room and with a private network for the equipment. AMP does not use eAuth. Access to AMP functions is controlled by ACF2 administered by the User Access Management Team (UAMT). For each component, individual frequently changed password-protected accounts are required. Login can only be performed by physical access to consoles within the AMP equipment room. Data is encrypted in transit and at rest, in compliance with USDA requirements on protecting information. Data is stored in a secure environment. Authorization is required to access the applications.

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?

- AMP – Information is used in financial and management reports, as well as loan servicing and customer notification correspondence.
- FOCUS – Produces reports from RD loan servicing and financial management data located on the DISC mainframe. FOCUS provides information with comprehensive features for entering, maintaining, retrieving, and analyzing data from loans and financial management data.

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.

- AMP – N/A, data is not analyzed.
- FOCUS – FOCUS itself is the tool that analyzes data and provides reports. FOCUS uses aggregate data from Guaranteed Loan System (GLS), Automated Multi-family Accounting System (AMAS), Program Loan Accounting System (PLAS), and Service Direct Loans (DLOS) also called Loanserv. FOCUS creates data snapshots for records retention (life of loan + 10yrs).

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 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

Controls are in place to erase memory in printers, remove media, internal traffic enhance protection, and protect the PII by keeping patches up to date. The equipment is in a secure environment where access is only granted to authorized personnel. Controls are in place to detect unauthorized access and audit logs are used to track user login activity. Authentication is used with the application and audit logs track user login activity.

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?

Notice is provided in the listed SORN, RD-1 SORN, 89 FR 72820, September 6, 2024.

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

Individuals cannot decline or opt out of the project this is covered by the initial points of collection.

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.

Mitigation

Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

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?

- AMP – PII information from the mail/print jobs are deleted from the print display in 24 hours and then deleted from archive at 60 days.
- FOCUS – Reports are not scheduled and therefore held permanently.

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.

- Automated Mail Processing (AMP) System N1-572-09-011
- Single Family Housing Records DAA-0572-2017-0001
- Audits and Investigations DAA-0572-2019-0001(FOCUS ties into these)

Privacy Impact Analysis: Related to retention of information.

Privacy Risk

HIGH RISK – The risk associated with maintaining data permanently in FOCUS is high, while risk is LOW for AMP as the PII information from the mail/print jobs are deleted from the print display in 24 hours and then deleted from archive at 60 days.

Mitigation

RD is in the process of scheduling system records for FOCUS directly. Until data retention is scheduled, the data is safeguarded in accordance with NIST 800-53 security controls.

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?

- AMP – AMAS, CLSS, GLS, LoanServ, MFIS – Loan information is submitted to AMP for the purpose of printing letters to program participants. Loan information is submitted to AMP through the use of software on the mainframe to create Print Stream. The software creates a Mail Run Data File (MRDF), a machine-readable barcode used by the insertion system for mail insertion, processing, and control purposes only.
- FOCUS – Shares financial management information with Farm Service Agency (FSA) to support loan and grant origination and processing and for business analysis, data trending, and data analytics in support of the RD mission. Transmit information electronically using encrypted data files.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk

MODERATE RISK Current risks are the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the borrower, if an individual, and on the tenant.

Mitigation

Data is stored in a secure environment. Access to the data is controlled by designated administrators, utilizing authentication. Data at rest and in transit is encrypted.

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?

- AMP – N/A
- FOCUS – Shares data with U.S. Department of Treasury Fiscal Service Treasury Web Application Infrastructure (TWA). BI provides debtor and debt information for Treasury Offset Program and Cross Servicing, which is done for federal agencies. TWA shares the full name, address information, and financial account information to TDW for the purpose of providing RD management with data to assist decision making. An Interconnection Security Agreement between TWA and USDA agencies, including RD, governs and authorizes the sharing of federal financial information, as well as Privacy Act data, from TWA into these USDA systems, including TDW.

Privacy Impact Analysis: Related to external sharing and disclosure.**Privacy Risk**

MODERATE RISK: Current risks are the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on the borrower, if an individual, and on the tenant.

Mitigation

Data is stored in a secure environment. Access to the data is controlled by designated administrators, utilizing authentication. Data at rest and in transit is encrypted.

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?

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

What are the procedures for correcting inaccurate or erroneous information?

The procedures for correcting inaccurate or erroneous information are listed in 7.1.

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

The listed SORN provides the procedures for notifying individuals of correcting their information.

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

Formal redress is provided.

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.

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?

The AMP equipment is secured by a multi-level, defense-in-depth approach. The equipment is housed in a specifically controlled room in a secure facility with physical access controls at both the facility and room levels. Network connectivity is secured with VLAN isolation of the AMP equipment room and with a private network for the equipment. AMP does not use eAuth. Access to AMP functions is controlled by ACF2 administered by the User Access Management Team (UAMT). For each component, individual frequently changed password-protected accounts are required. Login can only be performed by physical access to consoles within the AMP equipment room. Data is encrypted in transit and at rest, in compliance with USDA requirements on protecting information.

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

- AMP – System access procedures are documented, and access is managed by an authorized administrator under the System Security Plan (SSP) (AC-02, Account Management).
- FOCUS – The authorized administrator creates, modifies, and deletes user requests approved by the proper authority.

How does the program review and approve information sharing requirements?

Information sharing requests/requirements are reviewed annually.

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

All RD employees and contractors are required to complete annual information security and awareness training, which includes privacy training.