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	RD Midrange Moderate Applications 1
Program Office	N/A
Mission Area	USDA - RD
CSAM Number	2697
Date Submitted for Review	01/06/2026

Mission Area System/Program Contacts

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

Abstract

Midrange Moderate Applications Platform 1 (MMA1) is a newly created system of existing applications that have the security classification of moderate and are hosted on the USDA Digital Infrastructure Services Center (DISC) Midrange platform. This new system does not change any of the existing applications. The applications that process PII in MMA1 are Common Call Component (CCC), eForms, Business Intelligence (BI), and eServices.

Overview

Common Call Component (CCC) includes an application that processes PII Q-Action/Electronic Customer File (ECF)/Imaging is an internal document repository hosted on the USDA DISC Midrange platform. ECF/Imaging manages the electronic filing and retrieval of loan and grant documents for all Rural Development (RD) programs. ECF contains loan documents for multiple RD programs. ECF utilizes Q-ACTION to store, encrypt, and protect the documents while at rest. These documents, in many cases, contain PII. ECF/Imaging uses scanning software and equipment providing indexing, storage, and retrieval of electronic images of loan application documents and other paper requests sent to RD. ECF/Imaging uses, generates, and stores grant and loan images (documents) that contain PII.

eForms includes modules used by the public, program participants, and USDA employees. eForms was implemented to comply with the Paperwork Reduction Act and contains two (2) modules that process PII: MyForms, and Forms Admin. The eForms system contains two (2) modules that process PII: MyForms, and Forms Admin.

MyForms is an authenticated module that allows program participants to fill out and submit forms as part of their application package. The information collection process begins when program participants create an account on MyForms. After activating their account, program participants can download, complete, print, and deliver their forms through conventional mail or submit completed forms electronically through MyForms. Each package submitted is called an electronic service request that is routed to appropriate federal servicing offices for review. MyForms processes PII.

Forms Admin is an authenticated module that provides FPAC, AMS, and RD staff access to applications/packages submitted by program participants through MyForms. The electronic form is available in Forms Admin in a non-editable state. Program staff use Forms Admin to review and comment on applications. If any information is found to be missing/incorrect/ outdated, comments are added, and the form is reassigned to an editable state for participant correction in My Forms. New versions of forms are also introduced via the Forms Admin module. Forms Admin processes PII.

Business Intelligence (BI) is a combination of applications at USDA that processes information for business intelligence purposes to support RD mission needs such as loan servicing, business analysis, data trending, and data analytics. BI is an internal system that is not used or accessed by members of the public or non-federal entities. eFiche, Hyperion/EPM 11, TDW, and CXO Tableau process PII data. eFiche stores, reads, and retains reports generated by UDSA enterprise-level accounting and reporting systems and is capable of audit trails and allows the Government to maintain and research original documents. The purpose of eFiche is to allow USDA to search for stored information as well as the ability to perform selective printing, backup documentation and plans for offsite use. Access to eFiche is limited to authorized personnel. eFiche processes PII.

Hyperion/EPM11 are reporting tools used by RD staff. Enterprise Performance Management (EPM) is a Commercial-Off-the-Shelf (COTS) tool that provides RD employees reports as well as query and analysis capabilities. Hyperion/EPM11 provides real-time and historical reporting against TDW and against live data sources. Real-time data sources are PFCS, AASM, ECMS, and CLSS. RD staff must access Hyperion and user authorization is defined within the tool. Staff retrieve documents via the

web interface to view reports. EPM11 processes PII and a PII security group is in place to prevent unauthorized access.

The Data Warehouse (TDW) contains enterprise-wide data that is refreshed nightly from various on-line transactional processing (OLTP) systems. The data is cleansed, integrated, summarized and organized in a manner that is optimized for analytical and informational processing via OBIFS. The purpose of TDW is to provide critical business data in an expedient manner for RD decision-makers to sustain their respective program missions. Data in TDW is read-only and cannot be updated or changed by any user. TDW processes PII.

CXO Tableau provides RD users a platform to access reports, dashboards, and data sources published by the RD Technology Office, the RD Innovation Center, and other Tableau Creator and Explorer license holders. PII is processed. Access is limited to authorized personnel.

eServices System consists of a collection of webservices that support eGovernment initiatives and other RD systems. Each of these services provide RD staff with functionality to mask PII, verify accounts, process payments, transfer funds, and maintain federal reporting requirements with U.S. Treasury. The following applications process PII:

Account Cross Reference (ACR) is a secure webservice that provides masking and/or unmasking of Borrower Identification numbers (IDs) through a common lookup Tabular Data Warehouse (TDW) datastore. All communication is encrypted through Secure Socket Layer (SSL). ACR supports several request types: a borrower ID, multiple borrower IDs, a converted number representing a borrower ID, and multiple converted numbers representing corresponding borrower IDs. ACR processes PII from program participants and creates a spoofed number using a system algorithm. ACR is secure using E-Authentication.

Enterprise Cash Management System (ECMS) is the web view of the ECMS database, which currently holds disbursement, cash tracking and collection reconciliation information. ECMS processes PII, specifically full names, address information, SSN/Tax Identification Number (TIN), miscellaneous identification numbers, and borrower's banking account number(s) program participants, from LoanServ. ECMS access is role-based and secured using E-Authentication.

Electronic Funds Transfer (EFT) maintains a repository of bank accounts and routing information for payees who may receive disbursements for GLS, AMAS and PLAS. The information is used to support a disbursement when an EFT account is available for a payee. EFT uses an interface to add and maintain payees and their bank accounts. Disbursement processes for each of the systems interrogate EFT to determine if a given payee and payment type can have funds transferred directly via ACH. The routing information of financial institutions is maintained via a monthly file interface with Treasury. EFT is only used by RD staff and is secured using E-Authentication and application security. EFT processes PII.

Mortgage Account Information (MAI) provides online information to SFHD borrowers regarding their accounts with Rural Housing Service (RHS). MAI allows borrowers to make direct payments to RHS. MAI interfaces with LoanServ to validate accounts. MAI processes PII, specifically the borrower's full name, last 4 digits of SSN, financial data, and miscellaneous identification numbers from program participants. MAI is secured using E-Authentication.

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, as amended (P.L. 115-334)
- Consumer Credit Protection Act (15 USC 1601 et al)
- 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 10/23/24 and expires 10/23/27.

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

Midrange Moderate Platform 1 (MMA1) falls under SORN RD-1, Current or Prospective Producers or Landowners, Applicants, Borrowers, Grantees, Tenants and Other Participants in RD Programs

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 number
- File/Case ID number
- Truncated or partial social security number
- Taxpayer identification number
- Driver's license number
- Business taxpayer identification number (sole proprietor)
- Business bank account number (sole proprietor)

Biographical Information:

- Name (including nicknames)
- Ethnicity
- Citizenship
- Home address
- Spouse information
- Race
- Personal email address
- Employment information
- Business mailing address (sole proprietor)
- Business phone or fax number (sole proprietor)
- ZIP code
- Business email address
- Date of birth (MM/DD/YY)
- Home phone or fax number
- Marital status
- Personal finance information (including loan information)

Biometrics:

- Fingerprints
- Hair color

Distinguishing Features:

- Eye color
- Photos

- Signatures

Characteristics

- Height
- Weight

Specific Information/File Types:

- Case files
- Security clearance/Background check
- Civil/Criminal history information/Police record

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

- CCC System - ECF/Imaging - receives information from internal RD systems.
- eForms - Program participants provide their information directly on the forms.
- BI All data is derived from other internal systems.
- eFiche, Hyperion/EPM 11: receives information from internal RD systems.
- TDW: receives information from internal RD systems; as well as from an external source, U.S. Department of Treasury's Treasury Web Application Infrastructure (TWAI).
- eServices - receives information from internal RD systems.

How is the information collected?

- CCC - ECF/Imaging documentation is collected from RD internal applications or scanned in by authorized RD staff.
- eForms - MyForms and Forms Admin collect loans and grant application information directly from the applicant through electronic submission and/or through paper submission directly to staff offices for processing.
- BI and eServices are not the initial point of collection. All data is derived from other internal systems.

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

MMA1 does not use commercial sources or publicly available data.

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

- CCC and eServices are not the initial point of collection for PII information.
- eForms - Information is manually reviewed by authorized staff to verify the accuracy of the data as part of the standard workflow process.
- BI - eFiche, Hyperion/EPM11 and TDW data is checked internally by RD staff.

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.
- **Non-compliance with Regulations**: Failing to accurately characterize information can lead to non-compliance with privacy laws and regulations, resulting in legal penalties and reputational damage.
- **Inconsistent Handling Practices**: Without clear definitions and classifications, employees may handle PII inconsistently, leading to potential privacy violations.
- **Increased Risk of Data Breaches**: PII that is not properly characterized may not be prioritized for protection, making it more vulnerable to breaches and unauthorized disclosures.
- **Lack of User Awareness**: If individuals are not informed about how their PII is characterized and used, it can lead to a lack of trust and potential backlash against the organization.
- **Poor Incident Response**: Mischaracterized information can hinder effective incident response, as organizations may not recognize the sensitivity of the data involved in a breach.
- **Inadequate Training**: Employees may not receive proper training on handling specific types of data if the characterization is unclear, increasing the risk of errors in data management.
- **Failure to Honor User Rights**: Mischaracterization may lead to difficulties in fulfilling user rights requests, such as access or deletion, if the organization does not accurately track how data is categorized and used

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.
- **User Consent for Sensitive Data**: Obtain explicit consent for the collection and processing of sensitive personal information, such as health or financial data, and ensure that users are aware of its characterization.
- **Clear Definitions**: Establish clear definitions for different categories of personal information, helping employees understand how to classify and handle data appropriately.
- **Access Controls**: Implement access controls based on the classification of information, ensuring that only authorized personnel can access sensitive data.
- **Regular Training**: Provide training to employees on data characterization and the importance of handling PII according to its classification.
- **Documentation and Procedures**: Document procedures for the proper handling, storage, and sharing of different categories of personal information, ensuring compliance with privacy regulations.
- **Risk Assessments**: Conduct risk assessments for different categories of PII to identify potential vulnerabilities and develop mitigation strategies.

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?

- CCC - ECF/Imaging is an internal electronic document/file repository used by RD for processing loan and grant applications. Information is collected from RD internal applications or scanned in by authorized RD staff. ECF supports business purposes of is to introduce flexibility for RD Program Staff to retrieve loan and grant documents from a borrower level down to documents pertaining to a specific loan or grant.
- eForms - MyForms and Forms Admin processes information to allow for the collection of loan and grant applicant information related to the FPAC and RD loan and grant program. Information is collected directly from the applicant through electronic submission and/or through paper submission directly to staff offices for processing. eForms was developed for the purpose of complying with the Paperwork Reduction Act.
- BI - Information is collected from other RD systems for business intelligence purposes to support RD mission needs such as loan servicing, business analysis, data trending, and data analytics.
- eServices information is collected from other RD systems.
- ACR – masks SSNs to be used in other applications for the business purpose of minimizing the collection of SSN and de-identification.
- ECMS – information is used report required financial transaction to U.S. Treasury for the business purpose documenting disbursement activity.
- EFT – information is used to send an electronic funds transfer for RD service desk customers for the business purpose of ensuring timely transfer of funds from borrowers.
- MAI – PII information is used to validate accounts for the business purpose of enabling borrowers to schedule on-line loan payments.

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.

No

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk:

MODERATE RISK: Privacy act risks associated with the uses of information include:

- **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.
- **Overuse of Information**: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.
- **Loss of Data Control**: When PII is shared with third parties, there is a risk of losing control over how that data is used, potentially leading to unauthorized access or exploitation.
- **Increased Risk of Data Breaches**: The more PII is used and shared, the higher the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.
- **Inconsistent Application of Policies**: Variability in how different departments or employees apply data use policies can lead to privacy violations and confusion about acceptable practices.

Mitigation

- **Purpose Limitation**: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.
- **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.
- **Access Controls**: Implement access controls to restrict who can use personal information and for what purposes, ensuring that only authorized personnel have access to sensitive data.
- **Monitoring and Auditing**: Regularly monitor and audit the use of personal information to ensure compliance with privacy policies and identify any unauthorized or inappropriate uses.

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?

- CCC, BI, eServices – N/A. These systems are not the initial point of collection. Notice is provided to individuals by the initial source systems prior to collection or processing of the information.
- eForms – Yes, notice is provided on Form RD 410-4 to the individual prior to the collection of information when the individual applies for loans or grants.

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

- CCC, BI, eServices – N/A. These systems are not the initial point of collect where the opportunity to consent, decline, or opt out is provided.
- eForms – The Privacy Act Statement Required is provided directly on RD Form 410-4 where individuals are notified. Individuals have the opportunity and/or right to decline to provide information, but if they decline, then they will not be able to apply for loans or grants. To apply for an eForms loan or grant, the RD applicant consents to the collection of personal information as required for eForms loan or grant processing.

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.
- **Insufficient Updates**: Notices that are not regularly updated to reflect changes in data practices or legal requirements can mislead individuals and result in privacy violations.
- **Lack of Accessibility**: Notices that are not easily accessible or understandable to all individuals, including those with disabilities or language barriers, can lead to exclusion and non-compliance.
- **Failure to Communicate Changes**: Not adequately informing individuals about changes to privacy practices or policies can lead to confusion and mistrust, especially if data practices evolve.

- **Over-collection of Data**: If notices do not clearly explain the purpose of data collection, individuals may be more likely to provide information that is not necessary, leading to potential data minimization violations.
- **Inconsistent Messaging**: Different notices provided by various departments or mission areas may contain conflicting information, causing confusion and undermining trust.
- **Underestimating User Rights**: Notices that do not clearly outline individuals' rights regarding their personal information can prevent them from exercising those rights effectively.
- **Reputational Damage**: Poorly crafted or misleading notices can lead to public backlash, reputational harm, and loss of customer trust, affecting the departments/mission areas overall standing.

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.
- **Transparency**: Clearly outline what personal data is being collected, the purpose of data collection, how it will be used, and who it will be shared with.
- **Data Minimization**: Limit data collection to only what is necessary for the stated purpose. Avoid collecting excessive or irrelevant data.
- **User Rights**: Inform users about their rights regarding their personal data, including access, correction, deletion, and the ability to object to processing.
- **Training and Awareness**: Train employees on data protection practices and the importance of privacy notices to ensure compliance and proper handling of personal data.
- **Accessibility**: Make privacy notices easily accessible on websites and apps, ensuring they can be found without difficulty.
- **Feedback Mechanism**: Establish a process for users to ask questions or express concerns about privacy notices and practices, allowing for continuous improvement.

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?

- CCC – In addition to program area (SHF, MFH, CF, RUS, RBCS), there are classification structures for the following:
    - Servicing Office
    - Audited Financial Statements
    - Suitability
    - Civil Right
    - External Compliance Review
    - Office of Human Resources Management
    - Office of the Chief Financial Officer
    - Office of the Chief Information Officer
    - Office of the Chief Risk Officer
    - DAA-GRS-2016-0013-0001
    - DAA-GRS-2013-0003-0001
    - DAA-GRS-2013-0003-0011
    - DAA-GRS-2013-0003-0004
    - DAA-GRS-2015-0006-0001
    - DAA-GRS-2015-0006-0002
    - DAA-GRS-2015-0006-0003
    - DAA-GRS-2017-0007-0007
    - DAA-GRS-2018-0002-0010
    - DAA-GRS-2018-0002-0011
    - DAA-GRS-2016-0014-0001
    - DAA-GRS-2013-0006-0001
    - DAA-GRS-2013-0006-0002
    - DAA-05722019-0001-0008
    - DAA-0572-2017-0008-0004
    - DAA-GRS-2013-0008-0006
    - DAA-0572-2017-0008-0005
    - DAA-0572-2017-0008-0006
    - DAA-0572-2017-0008-0007
    - DAA-0572-2017-0008-0008
    - DAA-0572-2017-0005-0009
    - DAA-0572-2017-0001-0004
    - DAA-0572-2017-0001-0005
    - DAA-0572-2017-0001-0006
    - DAA-0572-2017-0001-0007
    - DAA-0572-2017-0001-0008

  - DAA-0572-2017-0005-0009
  - DAA-0572-2017-0001-0010
  - DAA-0572-2017-0007-0004
  - DAA-0572-2017-0007-0005
  - DAA-0572-2017-0007-0006
  - DAA-0572-2017-0005-0004
  - DAA-0572-2017-0005-0012
  - NC1-221-80-1 item 73
  - N1-221-08-1 item 4
  - N1-221-08-1 item 7b
- There are also unscheduled records in ECF for which records schedules in development will cover. These include:
  - RBCS Advanced Biofuels
  - RBCS Guaranteed Loans
  - Loan/Grant Combos for all programs
  - Unsuccessful funding applications for Electric and WEP, and RBCS RBIP Applications
- eForms – Single Family Housing records; 7yrs after cutoff.
- BI – The RD Records & Information Management Branch, in accordance with National Archives and Records Administration (NARA) federal policy and guidance, has evaluated and determined that the BI modules eFiche and TDW do not require a records schedule. The decision documentation is maintained by the RD Records Office. Hyperion/EPM 11 is unscheduled and therefore held permanently.
- eServices – no records are stored; schedule not required.

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.

- CCC – Partially (see 5.1).
- eForms – DAA-0572-2017-0001-0006 & DAA-0572-2017-0001-0004.
- BI – Partially (see 5.1).
- eServices – N/A

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.
- **Inadequate Disposal Procedures**: If agencies do not have secure methods for disposing PII that is no longer needed, it can lead to unintended exposure of sensitive data.

Mitigation

- **Data Retention Policy**: Use NARA data retention policies that outlines how long different types of PII will be retained and the rationale for those timeframes.
- **Regular Reviews**: 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.
- **Access Controls**: Implement strict access controls to limit who can view and manage retained personal information, reducing the risk of unauthorized access.
- **Data Minimization**: Collect and retain only the PII that is necessary for the intended purpose, minimizing the risk associated with holding excessive data.
- **Documentation and Training**: Ensure that employees are aware of and trained on the data retention policy, including the importance of compliance and the procedures for handling personal information.
- **Retention Schedule**: Follow a retention schedule that specifies the duration for retaining different types of records and when they should be reviewed or disposed of.
- **Audit Trail**: Maintain an audit trail to document when data is collected, accessed, and disposed of, which can help demonstrate compliance with retention policies.
- **Compliance Checks**: Regularly conduct compliance checks to ensure that retention practices align with legal requirements and organizational policies.
- **User Rights Notification**: Inform individuals about their rights regarding data retention, including the right to request deletion of their personal information when it is no longer necessary for the purposes for which it was collected.

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?

- CCC – ECF processes PII data from internal systems (RD and USDA) using scanning software and equipment to manage the electronic filing and retrieval of loan and grant documents for all RD programs.
- eForms – eForms does not share outside of RD. Forms are available for download to comply with the Paperwork Reduction Act.
- BI – information is transmitted internally within RD
- eFiche transmit PII via encrypted files to support loan and grant origination and processing and for business analysis, data trending, and data analytics
- Hyperion/EPM11 transmits PII via encrypted files to conduct data analysis.
- TDW transmits PII internally via encrypted files to support loan and grant origination and processing and for reports, query, and analysis.
- eServices –
- ACR receives requests from internal systems to mask/spoof SSN using HTTPS protocol
- ECMS receives PII from internal systems via HTTPS protocol to document the disbursement activity; the data transmitted to U.S. Treasury using SecureTransport like Connect: Direct (a batch job moves the files to the application servers).
- EFT receives PII from internal systems via HTTPS protocol to serve as a repository of customer banking information and to ensure timely transfer of funds from borrowers
- MAI receives PII from internal systems via HTTPS protocol to enable borrowers to schedule loan payments online.

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk

MODERATE RISK

- **CCC**: Current risks are associated with the potential unauthorized disclosure or illegal use of this PII and the potential adverse consequences this disclosure or use would have on program participants.
- **eFORMs**: eForms applications data retention has the potential risks of unauthorized access, unauthorized disclosure or illegal use of the RD customer PII data.
- **BI**: 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 program participants.
- **eServices**: The privacy risk is associated with unauthorized access and potential compromise of PII data.

Mitigation

- **CCC**: Data is stored in a secure environment. Access to the data is controlled by designated administrators, utilizing eAuthentication and Active Directory authentication to identify and authenticate the users. Data at rest and in transit is encrypted.
- **eForms**: Data is stored in a secure environment within the USDA. An eAuthentication account is required to access MyForms and Forms Admin.
- **BI**: Data is stored in a secure environment. Access to the data is controlled by designated administrators, utilizing eAuthentication and Active Directory authentication to identify and authenticate the users. Data at rest and in transit is encrypted.
- **eServices**: This privacy risk is 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.

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?

- CCC – N/A. ECF does not share data externally.
- eForms – N/A. eForms applications are not shared externally.
- BI - BI provides debtor and debt information with U.S. Department of Treasury Fiscal Service Treasury Web Application Infrastructure (TWAI), Treasury Offset Program and Cross Servicing. TDW receives the full name, address information, and financial account information from TWAI for the purpose of providing RD management with data to assist decision making.
- eServices - ECMS: ECMS sends the borrower's full name, bank account number, routing number, amount, account types, Treasury Account Symbol, and Business Event Type Code to U.S. Department of Treasury's Treasury Web Application Infrastructure's (TWAI) Pay.Gov. The purpose of the exchange is to route all agency collections to the correct treasury processing agent.

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk

- **Unauthorized Access**: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.
- **Data Breaches**: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.
- **Loss of Control**: Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

- **Non-compliance with Regulations**: Sharing PII without proper consent or outside the parameters set by privacy laws can result in legal penalties and reputational damage.
- **Inconsistent Data Management Practices**: Different third parties may have varying practices for handling PII, leading to inconsistencies in data protection and increased risks.
- **Insufficient Due Diligence**: Failing to conduct proper due diligence on third parties before sharing PII can expose mission areas to risks associated with partnering with unreliable or non-compliant entities.
- **Public Perception and Trust Erosion**: External sharing of PII, especially if not communicated transparently, can lead to public distrust and negative perceptions of the mission area or agency.
- **Reputational Damage**: If shared PII is misused or leads to negative outcomes for individuals, it can result in significant reputational harm to the mission area or agency responsible for the data.
- **Limited User Awareness**: Individuals may not be fully aware of how their PII is being shared or the potential risks involved, leading to a lack of informed consent.
- **Legal Liability**: Mission area and agency may face lawsuits or legal actions if individuals believe their PII has been mishandled or improperly disclosed, resulting in financial and operational impacts.

Mitigation

- **Data Sharing Policy**: Develop a clear policy outlining the conditions under which PII can be shared externally, including legal and compliance requirements (ex.: Computer Matching Agreements, SORNs, Business Agreements).
- **Due Diligence**: Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.
- **Written Agreements**: Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.

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?

- CCC, BI, eServices – These systems are not the initial point of collection; however, individuals may file a FOIAXpress request information or follow the record access procedures described in SORN RD-1.
- • eForms – Notification is part of the application process for eForms loan and grant applications, so the RD borrower/applicant can contact the appropriate RD staff member to correct any inaccurate information. RD applicants are prompted with the eForms application, itself, to correct errors as part of the application process. Also, RD staff involved in processing the loan or grant application do manual review and will contact the RD applicant for any information corrections with their application.

What are the procedures for correcting inaccurate or erroneous information?

- CCC, BI, eServices – These systems are not the initial point of collect where the opportunity to correct information is provided; however, individuals may file a FOIA request using RD FOIAXpress or follow the record access procedures described in SORN RD-1.
- eForms - Notification is part of the application process for eForms loan and grant applications, so the RD borrower/applicant can contact the appropriate RD staff member to correct any inaccurate information. RD applicants are prompted with the eForms application, itself, to correct errors as part of the application process. Also, RD staff involved in processing the loan or grant application do manual review and will contact the RD applicant for any information corrections with their application.

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

- CCC, BI, eServices – N/A. Individuals do not have access to these systems and are not the initial point of collect where individuals are notified on the procedures to correct information; however individuals may file a request using RD FOIAXpress or follow the record access procedures described in SORN RD-1.
- eForms - Individuals are notified of the procedure to gain access to and contest their information in the Record Access Procedures section as outlined in the SORN RD-1 under Record Access Procedures. RD applicants are prompted with the eForms application, itself, to correct errors as part of the application process.

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

- CCC, BI, eServices – N/A. Individuals do not have access to these systems and are not the initial point of collect where individuals are notified on the procedures to correct information; however individuals may file a request using RD FOIAXpress or follow the record access procedures described in SORN RD-1.

- eForms – N/A. 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.
- **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.
- **Failure to Address Complaints**: Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.
- **Delayed Responses**: Slow responses to redress requests can frustrate individuals and exacerbate feelings of mistrust and dissatisfaction, potentially leading to reputational harm.
- **Inconsistent Application**: If redress processes are applied inconsistently across different cases or agencies, it can lead to perceptions of unfairness and bias, undermining trust in the entire department.
- **Insufficient Recordkeeping**: Poor documentation of redress requests and outcomes can hinder an agency's ability to identify patterns of violations, learn from mistakes, and improve practices.
- **Legal Exposure**: Failing to provide adequate redress options may expose mission areas or agencies to legal challenges, including lawsuits or regulatory scrutiny, especially if individuals feel their rights have been violated.
- **Reputation Damage**: Public knowledge of inadequate redress mechanisms can damage the department's reputation, leading to loss of customer trust and potential business impacts.
- **Lack of Accountability**: Without effective redress mechanisms, mission areas or agencies may not be held accountable for privacy violations, which can perpetuate poor data handling practices.

Mitigation

- **Establish Clear Procedures**: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.
- **User Awareness Campaigns**: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.
- **Dedicated Privacy Officer/Privacy Point of Contact**: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.
- **Timely Response Protocols**: Implement protocols for acknowledging and responding to redress requests promptly, ensuring that individuals feel heard and valued.

- **Investigation Processes**: Create structured process for investigating redress requests, including gathering necessary information and documenting findings.

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?

- CCC – annual control assessments and continuous monitoring in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53. Access to ECF/Imaging is controlled through Level 2 eAuthentication, and access is controlled on a need-to-know basis for CCC.
- eForms – The NIST 800-53 controls for the eForms system access is controlled through Level 2 eAuthentication and monitored through event logging.
- BI – annual control assessments, and continuous monitoring in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53. Access to Hyperion/EPM 11 and TDW is controlled through Level 2 eAuthentication with audit logs of user activity for BI applications. eFiche access is controlled by Active Directory authentication.
- eServices – annual control assessments and continuous monitoring in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53. eServices applications follow USDA security and privacy requirements.

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

The RD process is accounting request and approval to the User Access Management desk procedures for each application.

How does the program review and approve information sharing requirements?

Information sharing with external partners is documented in formal Interconnect Security Agreements and approved by the RD system owner. These agreements are reviewed annually and re-signed every three (3) years when sharing will be continued.

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 complete annual USDA provided information security and awareness training, which includes privacy training.