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."
03/11/2025	1.5	Copy current FMMI PIA in Privacy review to the most current 608 compliant template per E.O.14168.

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Financial Management Modernization Initiative (FMMI)
Program Office	ACFO-SS
Mission Area	DAITO
CSAM Number	1053
Date Submitted for Review	03/12/2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Michele Washington	michele.washington@usda.gov	202-205-3369
Information System Security Manager	Kenneth B. McDuffie	Kenneth.mcduffie@usda.gov	504-982-6234
System/Program Managers	Linda A. Connolly	Linda.connolly@usda.gov	202- 674-9137

Abstract

The abstract provides the simplest explanation for the "what does the system do?" and will be published online to accompany the PIA link.

The Privacy Impact Assessment (PIA) describes the collection, use, processing, and dissemination of personally identifiable information (PII) by the Financial Management Modernization Initiative (FMMI) system. FMMI is USDA's enterprise-wide financial system that provides General Ledger, Management Funds, Management Fund Balance with Treasury, Payment Management, Receivables Management Cost Management, and Reporting services. This PIA is required by the E-Government Act of 2002 since FMMI processes, stores, and transmits PII data, as identified in the Privacy Threshold Analysis conducted for FMMI.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

System Name: Financial Management Modernization Initiative (FMMI)

USDA Component: Office of the Chief Financial Officer

Purpose: FMMI is USDA's enterprise-wide financial system that provides General Ledger Management, Funds Management, Fund Balance with Treasury, Payment Management, Receivables Management, Cost Management, Grants Management, and Reporting services. USDA agencies and components utilize FMMI for all Financial transactions executed by USDA, as well as requests for processing initiated by other Federal agencies.

Description: FMMI is a web-based solution providing access for all USDA financial users. FMMI has interfaces to other USDA financial systems, such as National Finance Center Payroll, Corporate Property Automated Information System (CPAIS), and Integrated Acquisition System. FMMI is built on the Systems, Applications, and Products (SAP) enterprise resource planning (ERP) Central Component (ECC) platform with modules for Financials, Controlling, Funds Management, Materials Management, and Sales and Distribution. In addition, FMMI utilizes SAP Business Warehouse (BW) for Reporting, SAP Customer Relationship Management (CRM) for grants management, SAP Process Orchestration (PO) for interfaces to other systems, and SAP Governance, Risk, and Compliance for enforcing Segregation of Duties controls. Enhanced functionality is provided using custom Reports, Interface, Conversion, enhancements, Forms and Workflows (RICEFW). The Pega application component with the FMMI SAP CRM solution allows grantees to search for grant opportunities, apply for grant opportunities, view agreement details, file claims, and receive status updates.

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.

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

Chief Financial Officers Act of 1990 (Pub. L. 101-576)

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

1. The Security Plan Status, **Complete**
2. The Security Plan Status Date, **2/24/2025**
3. The Authorization Status, Complete, **Re-authorized, 2/13/2025**
4. The Authorization Date, 8/21/2024, re-issue,
5. The Authorization Termination Date, 8/21/2027
6. The Risk Review Completion Date, **2/14/2025**
7. The FIPS 199 classification of the system (LOW/**MODERATE**/HIGH), 11***/28/2023.***

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

USDA/OCFO–10 Financial Systems.

1.4. 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.

2.1. 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. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers

☐ Social Security number	☐ Truncated or Partial Social Security number	☐ Driver's License number
☐ Passport number	☐ License Plate number	☐ Registration number
☒ File/Case ID number	☐ Student ID number	☐ Federal Student Aid number
☒ Employee Identification number	☐ Alien Registration number	☐ DOD ID number
☐ Professional License number	☒ Taxpayer Identification number	☒ Business Taxpayer Identification number (sole proprietor)
☐ Credit/Debit Card number	☐ Business Credit Card number (sole proprietor)	☐ Vehicle Identification number
☐ Business Vehicle Identification number (sole proprietor)	☒ Personal Bank Account number	☒ Business Bank Account number (sole proprietor)
☐ Personal Device Identifiers or Serial numbers	☐ Business Device Identifiers or Serial numbers (sole proprietor)	☐ Personal Mobile number

☐ Health Plan Beneficiary number	☒ Business Mobile number (sole proprietor)	☐ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)	☒ Business Mailing Address (sole proprietor)	☐ Date of Birth (MM/DD/YY)
☐ Ethnicity	☒ Business Phone or Fax Number (sole proprietor)	☐ Country of Birth
☐ City or County of Birth	☐ Group Organization/Membership	☐ Religion/Religious Preference
☐ Citizenship	☐ Immigration Status	☐ Home Phone or Fax Number
☒ Home Address	☒ ZIP Code	☐ Marital Status
☐ Spouse Information	☐ Children Information	☐ Military Service Information
☐ Race	☐ Nationality	☐ Mother's Maiden Name
☐ Personal Email Address	☒ Business Email Address	☐ Global Positioning System (GPS)/Location Data
☐ Employment Information	☐ Alias (Username/Screenname)	☐ Personal Financial Information (Including loan information)
☐ Education Information	☐ Resume or Curriculum Vitae	☐ Business Financial Information (Including loan information)
☐ Professional/Personal References		

Biometrics

☐ Fingerprints	☐ Hair Color	☐ DNA Sample or Profile
☐ Retina/Iris Scans	☐ Video Recording	

Distinguishing Features

☐ Palm Prints	☐ Eye Color	☐ Signatures
☐ Dental Profile	☐ Photos	

Characteristics

☐ Vascular Scans	☐ Height	☐ Weight
☐ Scars, Marks, Tattoos	☐ Voice/Audio Recording	

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)	☐ Cell Tower Records (e.g., Logs, User Location, Time)	☐ Network Communication Data

Medical /Emergency Information

☐ Medical/Health Information	☐ Mental Health Information	☐ Disability Information
☐ Workers' Compensation Information	☐ Patient ID Number	☐ Emergency Contact Information

Specific Information/File Types

☐ Personnel Files	☐ Law Enforcement Information	☐ Credit History Information
☐ Health Information	☐ Academic/Professional Background Information	☐ Civil/Criminal History Information/Police Record
☐ Case Files	☐ Security Clearance/Background Check	☐ Taxpayer Information/Tax Return Information

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

The two primary sources for data in FMMI are conversion from legacy systems and interfaces with external systems. Systems providing data for conversion to FMMI include:

- Government Online Accounting Link System (GOALS) II, Automatic Standard Application for Payment (ASAP) Invoice Processing Platform

- Financial Statements Data Warehouse (FSDW)
- Automated Cash Reconciliation Worksheet (ACRWS)
- Report on IPAC Transaction for Agriculture (RITA)
- Miscellaneous Income System (MINC)
- Program Loan Accounting
- Marketing and Regulatory Program
- Health and Human Services
- Grants and Awards, Grants.gov
- Forest Service Candidate Systems
- MeTTel
- Cooperative Research, Education and Extension Management
- Smart Pay 3
- Corporate Property Automated Information System (CPAIS)
- Integrated Acquisition System (IAS)
- Payroll/Personal System
- Administrative Billings and Collections System
- Lockboxes (US Bank)
- SAP Concur Cloud for Public Use
- mLINQs (move LINQ-USDA)
- FPAC Source Systems
- US Treasury TWAI

2.2.1. How is the information collected?

FMMI data is collected from all USDA agencies' accounting and budget execution transactions or directly entered into FMMI by users assigned to financial administration roles. Additionally, Pega users enter information regarding grants and agreements with grantees.

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

No.

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

Data received by FMMI requires a highly concise format consistent with other USDA financial systems. Data not in the proper format will trigger an alert for auditors to examine. Data that is properly formatted but contains erroneous numbers, misspellings, etc., will fail automated checks applied by the system. These failures will also trigger an alert for auditors to examine. External agencies implement additional checks for accuracy, including transaction integrity checksums. We check

processed record counts against expected values to ensure all transactional processes have been completed.

2.5. Does the system/program use third-party websites?

Not applicable

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

Not applicable.

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

Not applicable.

2.6. **Privacy Impact Analysis**: Related to characterization of the information.

Follow the format below:

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

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: By Implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

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.

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.

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

Financial planners and managers use FMMI data for financial planning and management, to make payments, award grants, and report to government agencies like Treasury and the OMB for budget execution, cash disbursements, and other financial obligations.

3.2. 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.

FMMI utilizes the SAP Governance, Risk, and Compliance (GRC) Access Control product to supplement the core security provided by SAP and Pega. Specifically, GRC provides functionality to ensure that segregation of duty (SoD) conflicts is not introduced into the system. GRC is configured to run in preventative mode to prevent these conflicts from occurring. Within the GRC Access Control the following components handle access provisioning and SoD conflicts:

- Access Risk Analysis (ARA)
- Emergency Access Management (EAM)
- Access Request Management (ARM).

The Access Control tool handles FMMI provisioning across ECC, BW, Portal, CRM, Solution Manager, PO, and the GRC system for end users and the project support team members. FMMI Portal is the single Point of Entry for all FMMI applications including GRC Access Control.

3.3. **Privacy Impact Analysis**: Related to uses of the information.

Follow the format below:

Privacy 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.

Mitigation: By Implementing some or all the following mitigation actions, mission areas may better safeguard PII and ensure responsible use in compliance with PA requirement:

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.

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.

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

The U.S. Governments intention to collect PII data is declared in various System of Record Notices made publicly available within the U.S. Federal Register, as well as in the Privacy Act, and at data collection points throughout the Federal Government. Individuals who enter their own PII data are notified of their rights and protections under the Privacy Act before providing the information, which are outside the span of control of the USDA ACFO-SS/FMS. FMMI does not directly request PII data from individuals as part of its routine operations.

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

Individuals have the right to decline providing information, based upon protections and limitations in various US Regulations, Acts, guidelines, and policies at each point of collection. FMMI does not directly request PII data from individuals as part of its routine operations.

Individuals consent to use the information at the time of provision. Grievances involving consent and unauthorized use of the information can be addressed to the collection Government agency, to agencies listed within the applicable System of Record Notice, or through other legal means.

4.3. **Privacy Impact Analysis**: Related to notice.

Follow the format below:

Privacy Risk: Privacy Act risks associated with notices include:

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: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act requirements:

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.

5.1. What information is retained and for how long?

FMMI data is retained by ACFO-SS/FMS following the National Archives and Record Administration (NARA) guidelines provided in the General Records Schedule 1.1, Financial Management and Reporting Records.

5.2. 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. Records are retained in accordance with NARA policies, USDA DR 3080-001, Records Management, USDA DR-3090, Litigation Retention Policy for Documentary Materials including Electronically Stored Information, et al. and General Records Schedule 1.1, Financial Management and Reporting Records.

.

5.3. **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: Privacy act risks associated with the retention of information include:

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 are no longer needed, it can lead to unintended exposure of sensitive data.

Mitigation: By implementing the following mitigation actions, mission areas can ensure responsible retention of PII while complying with the PA.

Data Retention Policy: Use NARA data retention policies that outline 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.

Section 6: Information Sharing

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

6.1. 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?

The FMMI system, operated on behalf of the USDA by ACFO-SS/FMS shares information with other USDA systems operated by the Office of Procurement and Property, the National Finance Center, and the Research, Education and Economics mission within the Office of Chief Scientist. PII data relevant to financial transaction processing is shared with these internal USDA organizations. Information may be shared with senior leadership across USDA through a series of Tableau dashboards and reports for the purpose of promoting data-driven decisions. The information shared will span data from different various administrative domains IT, Finance, HR, Property, Operations, Homeland Security, and Property.

Information is shared almost exclusively via electronic file transfer. Security measures implemented to protect the electronic sharing of information amongst USDA agencies are described in the FMMI Interconnection Security Agreements. Manual data sharing (CD, hardcopy, etc.) is permitted only in rare and special circumstances. The information will be transmitted to the USDA Data Lake via security file transfer methods such as Security File Transfer Protocol (SFTP) and Web Services. Once in the USDA Data Lake, data will be shared via a series of Tableau dashboards.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: There are risks associated with the internal sharing of PII data amongst USDA agencies, such as unauthorized personnel viewing PII, PII data spillage, and data being intercepted during transit.

Mitigation: All personnel accessing FMMI PII data are cleared and trained annually on the proper handling and protection of PII data. The FMMI system is protected by role-based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so within the application boundary. The risk of sharing data within USDA is considered low-moderate. Network encryption protocols ensure PII is not inadvertently shared in an unencrypted format. FMMI data is encrypted in motion and at rest. In addition, access to data is limited to only those people with a need-to- know by using an internal, granular governance process. Dissemination of information is governed by internal USDA policy.

6.3. 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?

FMMI financial and PII data is shared with the following organizations, for the purpose of accurate accounting transactions:

- Department of the Treasury, for monetary disbursements.
- Internal Revenue Service, for tax reporting and collection
- Office of Management and Budget, for USDA financial Reporting
- Grants data is shared with external grantees for the purpose of awarding and status

Information is shared exclusively via electronic file transfer. Manual data sharing (CD, hardcopy, etc.) is permitted by submitting a formal request to the ACFO-SS/FMS Director describing the reason for requiring manual data instead of electronic transfer. All FMMI interconnections are safeguarded through security measures defined within established MOU or ISA. Security controls applied to system interconnections are regularly assessed to verify and validate that security protections are operating as intended.

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

Follow the format below:

Privacy Risk: Privacy risks associated with external sharing and disclosure include:

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.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

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.

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

Individuals may obtain information regarding the procedures for gaining access to their own records contained within FMMI by submitting a request to the Privacy Act Office, 1400 Independence Avenue, SW, South Building, Washington, DC 20250. The envelope, and letters contained therein, should bear the words "Privacy Act Request." A request for information should contain the name of the individual, the individual's correspondence address, the name of the system of records, the year(s) of the records in question, and any other pertinent information to help identify the file(s). FMMI users can also place a Service Now (SNOW) ticket for a review of any incorrect privacy information on a person by proper FMS personnel.

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

Procedures for contesting records are the same as procedures for record access in section 7.1 above. Include the reason for contesting the record and the proposed amendment to the information, including any supporting documentation that shows how the record is inaccurate.

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

The system of records notice in the Federal Register provides notification. Procedures for contesting records are the same as procedures for the record access in section 7.1. Include the reason for contesting the record and the proposed amendment to the information, including any supporting documentation that shows how the record is inaccurate.

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

If formal redress is impossible after contacting USDA following established procedures, individuals should pursue other legal options to correct erroneous information, such as filing a civil and/or criminal complaint.

7.5. **Privacy Impact Analysis**: Related to redress.

Follow the format below:

Privacy Risk: Privacy Act risks associated with redress include:

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.

Mitigation: Implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

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.

Section 8: Auditing and Accountability

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

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

FMMI logs all access to sensitive PII data. These logs are reviewed weekly for indications of misuse. The VFC **(Amazon AWS East/West by mid / late 2025)** hosting environment provided real-time monitoring of networked connections and data flow. User accounts are re-authorized for continued need and applicability.

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

Individuals may obtain information regarding the procedures for gaining access to their own records contained within FMMI by submitting a request to the Privacy Act Office, 1400 Independence Avenue, SW, South Building, Washington, DC 20250. The envelope, and letters contained therein, should bear the words "Privacy Act Request." A request for information should contain the name of the individual, the individual's correspondence address, the name of the system of records, the year(s) of the records in question, and any other pertinent information to help identify the file(s).

8.3. How does the program review and approve information sharing requirements?

Information is shared exclusively via electronic file transfer. Manual data sharing (CD, hardcopy, etc.) is permitted by submitting a formal request to the ACFO-SS/FMS Director describing the reason for requiring manual data instead of electronic transfer. All FMMI interconnections are safeguarded through security measures defined within established MOU or ISA. Security controls applied to system interconnections are regularly assessed to verify and validate that security protections are operating as intended.

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

All users take the USDA Security and Awareness Training when they are onboard and retake the training annually. This training covers PII and its need for safeguarding. Privileged users also take a more in- depth training course commensurate with their access permissions. If an incident occurs with PII, the user must take a course in PII available on AgLearn.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 4/28/2025

USDA Privacy Analyst (On behalf of USDA's Chief Privacy Officer):

Signed:_____

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Signed:_____

Linda A. Connolly, System
Owner Deputy Director,
Financial Management Services
United States Department of
Agriculture

Signed: _____

Privacy Officer, Departmental
Administration Information
Technology Office (DAITO)
United States Department of
Agriculture

Signed TRACY HENDRIX Digitally signed by TRACY HENDRIX Date: 2025.05.08 18:28:36 -04'00'

Chief Privacy Officer
United States Department of Agriculture