U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

2023

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

Reporting of Intra-governmental Payments and Collections (IPAC) Transactions from Agriculture (RITA)

Associate Chief financial Officer – Shared Services (ACFO-SS)

Financial Management Services (FMS)

Date PIA submitted for review:

November 26, 2024

Mission Area System/Program Contacts:

	Name	**E-mail**	**Phone Number**
Mission Area Privacy Officer	Michele Washington	Michele.washington@usda.gov	(202) 205-3369
Information System Security Manager	Kenneth McDuffie	Kenneth.mcduffie@usda.gov	(504) 982-6234
System/Program Managers	Linda Connolly	Linda.Connolly@usda.gov	(202) 674-9137

Abstract
The U.S. Department of Treasury (Treasury) hosts the Intra-Governmental Payment and Collection Systems (IPAC) to provide a standardized interagency fund transfer mechanism for use by Federal agencies. IPAC facilitates the intra-governmental transfer of funds, with descriptive data, from one agency to another. IPAC communicates changes in the status of funds to agencies in the form of bulk files.

The Reporting of IPAC Transactions from Agriculture (RITA) is a major mission supportive web-based application. RITA monitors the processing of Intra-governmental Payments and Collections (IPAC) payments and collections that reference USDA Agency Location Codes (ALC). RITA reconciles the IPAC intra-governmental transactions from Treasury to the related USDA financial management system transactions to identify any unprocessed IPAC intra-governmental transactions. It tracks the status and records the history of the unprocessed IPAC intra-governmental transactions (IPAC bills'). Users can view the bill details, including processing history, assignment history and notes history in RITA. RITA produces reports on IPAC transactions. These reports include the ability to print bills, ageing reports, and management reports.

IPAC sends all unprocessed transactions to USDA through RITA.

Overview
The United States Department of Agriculture (USDA) Office of the Chief Financial Officer (OCFO) Associate Chief Financial Officer for Shared Services, Financial Management Services (ACFO-SS/FMS) is the organization responsible for the security, operation and maintenance of the RITA application. The RITA infrastructure is hosted by Virtustream Federal Cloud (VFC), a FedRAMP approved Cloud provider. The primary computing facility is in the state of Virginia. The backup computing facility is in the state of Pennsylvania. Physical and environmental controls are provided as part of hosting services, and established Service Level Agreements (SLAs) and Contracts between ACFO-SS/FMS and VFC. It is the responsibility of VFC to provide the disaster recovery and reconstitution of the RITA infrastructure as well as the general support environments. The hosting provider, VFC, is responsible for the general support environment and the RITA infrastructure.

RITA is a Cloud and web-based database management system that integrates fiscal activity for interagency billings from both Treasury and USDA agencies. The system categorization is Moderate. USDA's eAuthentication (eAUTH) solution serves as the centralized authentication service for USDA employees to access USDA Web Services, including access to the RITA application.

Section 1.0 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 System of Records Notice(s) (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)

RITA collects information related to IPAC intra-governmental funds transfers received from Treasury, and subsequent General Ledger activity that substantiates recordation of the Treasury fund transfer in USDA's financial management systems, Financial Management Modernization Initiative (FMMI) and Central Accounting System (CAS). RITA disseminates IPAC intra-governmental funds transfers received from Treasury to USDA financial management systems (FMMI and CAS) to enable recordation of the Treasury fund transfers.

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

Security Assessment and Accreditation for RITA was completed in Fiscal Year (FY)2022. The fiscal year annual testing was conducted for FY23 and FY24 during 2024. FY25 will be the year RITA is re-accredited in accordance with USDA Risk Management Framework Process.

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

USDA/OCFO-10, Financial Systems – 83 FR 67712 (December 19, 2018)

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

No

Section 2.0 Characterization of the Information

Authorized USDA personnel use Personally Identifiable Information (PII) to associate IPAC intra-governmental funds transfers and amounts with authorized expenditures, and to contact corporate and individual representatives when questions arise.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

RITA collects information related to IPAC intra-governmental funds transfers received from Treasury, and subsequent General Ledger activity that substantiates recordation of the Treasury fund transfer in USDA's financial management systems (FMMI and CAS). RITA disseminates IPAC intra-governmental funds transfers received from Treasury to USDA financial management systems (FMMI and CAS) to enable recordation of the Treasury fund transfers.

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	☐	License Plate Number
☐	Registration Number	☐	File/Case ID Number

☐	Student ID Number	☐	Federal Student Aid Number
☐	Passport number	☐	Alien Registration Number
☐	DOD ID Number	☐	DOD Benefits Number
☐	Employee Identification 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	☐	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number		

Biographical Information

☒	Name (including nicknames)	☐	Sex	☐	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
☐	Citizenship	☐	Immigration Status	☐	Religion/Religious Preference
☐	Home Address	☐	Zip Code	☐	Home Phone or Fax Number
☐	Spouse Information	☐		☐	Children Information
☐	Marital Status	☐	Military Service Information	☐	Mother's Maiden Name
☐	Race	☐	Nationality	☐	Global Positioning System (GPS)/Location Data
☐	Personal e-mail address	☐	Business e-mail address	☐	Personal Financial Information (including loan information)
☐	Employment Information	☐	Alias (username/screenname)	☐	Business Financial Information (including loan information)
☐	Education Information	☐	Resume or curriculum vitae	☐	Professional/personal references

Biometrics/Distinguishing Features/Characteristics

☐	Fingerprints	☐	Palm prints	☐	Vascular scans
☐	Retina/Iris Scans	☐	Dental Profile	☐	Scars, marks, tattoos
☐	Hair Color	☐	Eye Color	☐	Height
☐	Video recording	☐	Photos	☐	Voice/ Audio Recording
☐	DNA Sample or Profile	☐	Signatures	☐	Weight

Medical/Emergency Information

☐	Medical/Health Information	☐	Mental Health Information	☐	Disability Information

☐	Workers' Compensation Information	☐	Patient ID Number	☐	Emergency Contact Information
Device Information					
☐	Device settings or preferences (e.g., security level, sharing options, ringtones)	☐	Cell tower records (e.g., logs, user location, time, etc.)	☐	Network communications data
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 information in the system/program?

The PII within the system is transferred by the Department of Treasury Intra-Governmental Payment and Collection System (IPAC) in the form of General Ledger reports. The reports contain individuals' full name and social security numbers.

USDA financial management systems (FMMI and CAS) provide transactions that validate recordation of the Treasury IPAC fund transfers.

*Centralized Accounting System (CAS) is operated and is the responsibility of the OCFO-National Finance Center (NFC).

The name and SSN are provided in the ledger report to validate the funds being transferred back to USDA from the Department of Treasury due to the USDA funds not being disputed by the payee within 15 months.

2.2.1. How is the information collected?

The information is collected through the Department of Treasury IPAC system. The General Ledger bulk file reports compile the data in which unprocessed funds dispersed by USDA via check are returned to USDA electronically by the Department of Treasury.

The ledgers are retrieved by authorized USDA ICB staff from Treasury's IPAC website (https://ipac.fms.treas.gov).

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

Not applicable. RITA does not use commercial or publicly available data.

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

RITA applies a broad range of data type, length, and enumerated value edits during initial data imports. Additional edits are applied prior to final acceptance of data to detect data consistency and duplication errors. Database foreign keys and other data constraints are defined as a further safeguard to assure data accuracy and completeness.

RITA validates the uniqueness of each transaction by comparing its bill number and bill date to the bill number and bill date stored in RITA every day. All of the fields have a set of valid values that can be specified. These values should be fairly obvious - such as the numbers 0 to 59 for seconds and minutes, and the values 0 to 23 for hours. Day-of-Month can be any value 1-31.

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

No

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

RITA does not utilize third-party websites.

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

Not applicable. RITA does not utilize third-party websites.

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.

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.
Mitigation: Addressing risks through proper data characterization practices is essential for maintaining compliance with the PA and protecting individuals' personal information. By Implementing 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.

Access Controls: Implement access controls based on the classification of information, ensuring that only authorized personnel can access sensitive data.

Risk Assessments: Conduct risk assessments for different categories of PII to identify potential vulnerabilities and develop mitigation strategies.
Monitoring and Auditing: Regularly monitor and audit data practices to ensure compliance with classification policies and identify any misclassification or improper handling of information.

Section 3.0 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?

Names and SSNs are transferred from the Department of Treasury's IPAC system to RITA via the ledger log to track funds paid by USDA to individuals through the Treasury. If the disbursed funds remain unnegotiated for 15 months, the Treasury will refund the money to USDA. The IPAC system then generates a ledger detailing the refund source, which is used for balancing and reconciling agency accounts.

RITA assures that Treasury and USDA financial system fund balances are consistent with one another. RITA identifies inconsistencies as unreconciled or partially reconciled bills.

RITA additionally assigns unreconciled activity to USDA technicians for research and resolution, and aids technicians and agency personnel in reconciling agency and Treasury data with a variety of management tools and reports.

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.

RITA utilizes Online Analytical Processing (OLAP) – is a computer-based technique that analyzes large amounts of data to generate business insights. OLAP is used in business intelligence (BI), decision support, and reporting. OLAP uses multidimensional arrays of data called OLAP cubes to perform complex queries and multidimensional analysis. RITA uses the Saiku/Mondrian OLAP tool to provide users with a means of identifying trends and high-level characteristics related to their effectiveness in reconciling IPAC intra-governmental funds transfers. Saiku cube dimensions and measures exclude all data elements that may include PII.

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.

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.

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

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.

Section 4.0 Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to use 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?

USDA/OCFO-10 SORN, Financial Systems, provides the notice for the collection of information.

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

Individuals have the right to decline to provide their information at the point of origin of the information.

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.

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.

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.

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.

Section 5.0 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?

Names and social security numbers are retained in RITA 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.

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.

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

Mitigation: 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 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.

Section 6.0 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 information in RITA is shared with the following systems within USDA:

- Administrative Billings and Collections Systems
- Automated Cash Reconciliation Worksheet System
- Federal Cloud (VFC)
- Financial Management Modernization Initiative
- ICAM Shared Services

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Disclosure of PII could cause serious harm to the agency mission, to the associated personnel, and could result in litigation.

Mitigation: To ensure the protection of the data when shared internally RITA implements the following security control:

Encryption – All client/server communications are encrypted through Transport Layer Security.

Masking of PII data – Users may view data or report data that includes PII only if they are assigned a PII viewing role. For users without the PII role, RITA performs a pattern search on all data fields that may contain PII and replaces PII data patterns with a series of X characters. PII masking occurs within the database prior to delivering query results and is effective for all forms of access. PII is masked for RITA application access, for all forms of reporting, and for ad-hoc query.

Controlled access – USDA eAuthentication limits RITA access to authorized users only. In addition, authorized users must be defined to the RITA application.

Timeout for remote access – RITA sessions are cancelled by the application server after a specified idle period.

System audit logs – RITA captures and retains all logon and logoff actions, and selected additional actions such as changes to user profiles.

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?

RITA does not share data outside of USDA.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.
Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 7.0 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 seeking to gain access to their information contained in this system may submit a request in writing to Departmental FOIA Officer who can be contacted by email at usdafoia@usda.gov or at 1400 Independence Avenue SW, Room 4039-A, Washington, DC 20250.

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

Individuals seeking to correct inaccurate or erroneous information contained in this system may submit a request in writing to Departmental FOIA Officer who can be contacted by email at usdafoia@usda.gov or at 1400 Independence Avenue SW, Room 4039-A, Washington, DC 20250.

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

Individuals are notified of the procedures for correcting their information through the OCFO–10'USDA/OCFO-10 System of Records Notice which is published in the Federal Register.

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

N/A. Formal redress is provided.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk:

Procedures for individuals accessing their personal information, correcting inaccurate or erroneous data, and receiving notification of these correction are in place at USDA.

Mitigation:

The SORN outlines clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

Users are informed about their rights under the privacy act and the available redress mechanisms through the SORN.

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?

The information in the system is secured through:

•Encryption – All client/server communications are encrypted through Transport Layer Security.

• Masking of PII data – Users may view data or report data that includes PII only if they are assigned a PII viewing role. For users without the PII role, RITA performs a pattern search on all data fields that may contain PII and replaces PII data patterns with a series of X characters. PII masking occurs within the database prior to delivering query results and is effective for all forms of access. PII is masked for RITA application access, for all forms of reporting, and for ad-hoc query.

• Controlled access – USDA eAuthentication limits RITA access to authorized users only. In addition, authorized users must be defined to the RITA application.

• Timeout for remote access – RITA sessions are cancelled by the application server after a specified idle period.

• System audit logs – RITA captures and retains all logon and logoff actions and selected additional actions such as changes to user profiles.

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

Users have access to the information in the system based on job function and the need to know the information. Security profiles are set up for users to ensure that internal controls and separation of duties are maintained. Sensitive information is restricted from users if there is no valid job-related need for the information to perform the duties of their position.

A Corporate Systems Access Request Form (AD-1143) is required to establish a user account, report a change in duties, report separation from the agency, and report name or profile changes.

For agency personnel, the user's supervisor must review and approve the Corporate Systems Access Request Form and forward it to an agency coordinator for review and approval. The agency coordinator signs the form and forwards it to the IPAC Control Branch (ICB) for additional approval. ICB approved forms are forwarded to the RITA User Management point of contact that is responsible for adding, updating, or deleting the user as specified on the form.

For ICB staff, the user's supervisor must review and approve the Corporate Systems Access Request Form and forward it to an ICB coordinator for review and approval. The ICB approved forms are forwarded to the RITA User Management point of contact that is responsible for adding, updating, or deleting the user as specified on the form.

The system developers have access to maintain the system databases and files. The system developers also have appropriate access to view the data to ensure it is correct. Access is only granted after appropriate background investigations have been completed.

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

Authorized USDA agency users access RITA in the same way as ACFO-SS/FMS internal users. Limitations are applied through the assignment of restrictive roles.

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

All users, including contractors, are required to complete privacy training and it is provided to appropriate RITA personnel before authorizing access to the system and annually thereafter. Training includes basic security briefings about awareness training and annual refresher training, rules of behavior, and non-disclosure agreements.

Users sign the documents acknowledging that they have read and understood the system security rules and must sign a document confirming that they understand the rules. All government employees and contractors' complete security basics and privacy training annually before access is granted. These documents are kept on file with original signatures. All users training is tracked and reported through AgLearn and via the RITA monthly scorecard. Personnel identified as having system security roles and responsibilities are provided additional specialized training through AgLearn.

Approval Signatures:

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

_____
Mission Area Privacy Officer
Departmental Administration Information
Technology Office, DAITO
United States Department of Agriculture

_____
Sullie Coleman, CISO/ACISO
Departmental Administration Information
Technology Office, DAITO
United States Department of Agriculture

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.05.01 17:04:28 -04'00'

_____
Officer of the Chief Privacy Officer
United States Department of Agriculture