Privacy Impact Assessment

Technology, Planning, Architecture, & E-Government

- Version: 2.0
- Date: April 2019
- Prepared for: USDA OCFO-FMS RITA

United States Department of Agriculture

Privacy Impact Assessment for the

Reporting of IPAC Transactions from Agriculture RITA

April 2019

Contact Point

Linda Connolly
Director of OCFO/FMS/TISD
Office of the Chief Financial Officer for Financial Management Services (OCFO-FMS)
United States Department of Agriculture
(202) 674-9137

Reviewing Official

Stanley McMichael
System Owner
Office of the Chief Financial Officer for Financial Management Services (OCFO-FMS)
United States Department of Agriculture
(202) 720-0564

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.

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 are able to 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, aging reports, and management reports.

Overview

The Chief Financial Officer for Financial Management Services (OCFO-FMS) is the organization responsible for the security, operation and maintenance of the RITA application. The RITA infrastructure is hosted by Virtustream Federal Cloud, 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 OCFO-FMS and Virtustream Federal Cloud. It is the responsibility of Virtustream Federal Cloud to provide the disaster recovery and reconstitution of the RITA infrastructure as well as the general support environments. The hosting provider, Virtustream Federal Cloud**,** will first establish the general support environments 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 Characterization of the Information

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

1.1 What information is collected, used, disseminated, or maintained in the system?

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.

1.2 What are the sources of the information in the system?

Treasury provides IPAC intra-governmental funds transfers as bulk files. These files are retrieved by authorized USDA ICB staff from Treasury's IPAC website (https://ipac.fms.treas.gov).

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

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

1.3 Why is the information being collected, used, disseminated, or maintained?

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.

1.4 How is the information collected?

Treasury provides IPAC intra-governmental funds transfers as bulk files. These files are retrieved by authorized USDA ICB staff from Treasury's IPAC website (https://ipac.fms.treas.gov).

USDA financial systems provide General Ledger data as bulk files. These files are transferred to server accessible staging directories by USDA financial management systems using secure file transfer processes.

1.5 How will the information be checked for accuracy?

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.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Social Security Act, Internal Revenue Services, Treasury, Office of Management and Budget.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Collected information is related to IPAC intra-governmental funds transfers. Treasury IPAC bulk file transactions may include corporate and individual TINs and SSNs (PII). These PII are provided by Treasury to aid in identifying the origin and purpose of intra-governmental funds transfers. Authorized USDA personnel may subsequently use this information to associate IPAC intra-governmental funds transfers and amounts with authorized expenditures, and to contact corporate and individual representatives when questions arise.

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

These risks are mitigated by applying the following controls:

- 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.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

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

2.2 What types of tools are used to analyze data and what type of data may be produced?

RITA users may employ both highly customized and general purpose tools to analyze

data:

- RITA web application – The RITA web application and its related webpages present users with Treasury and GL transaction details. For users granted a PII role, this information may include PII. All other users (i.e., those without a PII role) RITA replaced PII with a series of X characters.
- Reporting – RITA uses the JasperReports Library reporting tool to produce a variety of summary and detail level reports. Reports may be scheduled for regular publication and delivery via email, or may be requested for on-demand publication. PII masking is always applied to on-demand reports publication. PII masking is not applied for on-demand publication if the user requesting the report is assigned the PII role.
- Online Analytical Processing (OLAP) – 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.
- Ad-hoc Reporting – RITA users may be provided access to ad-hoc reporting tools. The RITA PII masking implementation prevents access to PII from outside the RITA application.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

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

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

RITA maintains NIST and USDA prescribed interconnection system agreements (ISAs) to protect information being transferred into or out of the RITA system. Access controls including role-based account management and implementation of separation of duties and least privilege is enforced by the RITA system through the use of roles and profiles. RITA predefines roles that limit access to viewing and update capabilities. These role are then grouped into profiles. Each RITA user is assigned a profile that limits the user's access.

The RITA system is authorized to operate in accordance with compliance to NIST, FISMA and USDA security requirements. RITA does not use commercial or publicly available data.

Section 3.0 Retention

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

3.1 How long is information retained?

Information is retained in compliance with NARA retention guidelines for financial management data. Bill related data is retained for a minimum of six full years.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention period has been approved by the component records officer and the National Archives and Records Administration (NARA).

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Longer period of data retention can impose the risk of data being stolen, loss of data integrity and confidentiality. OCFO-FMS has implemented security controls to protect data.

Information is protected by access rules. Users who need access to the data must be granted access by an authorized individual and will apply the appropriate access rules to the user's ID.

Users are required to undergo training and sign a document of understanding.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

USDA agency financial managers are tasked to reconcile their agency's status of funds with Treasury. Agency financial managers task staff members to support IPAC Control Branch efforts to resolve unreconciled funds transfers. Agency staff members are granted RITA access in a restricted capacity to research and resolve their agencies status of funds.

4.2 How is the information transmitted or disclosed?

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

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Collected information is related to IPAC intra-governmental funds transfers. Treasury IPAC bulk file transactions may include corporate and individual TINs and SSNs (PII). These PII are provided by Treasury to aid in identifying the origin and purpose of an intra-governmental funds transfer. Authorized USDA personnel may subsequently use this information to associate IPAC intra-governmental funds transfers and amounts with authorized expenditures, and to contact corporate and individual representatives when questions arise.

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

These risks are mitigated by applying the following controls:

- 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.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

Not Applicable. No RITA data is shared outside of the USDA.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Not applicable. No RITA data is shared outside of the USDA.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Not applicable. No RITA data is shared outside of the USDA.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Not applicable. No RITA data is shared outside of the USDA.

Section 6.0 Notice

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

6.1 Was notice provided to the individual prior to collection of information?

RITA is a reporting tool that receives downloads from the FMMI ledger and Treasury. The OCFO-10 SORN, *Financial Systems,* provides the notice that the USDA will retain this information and it provides contact information.
https://www.federalregister.gov/documents/2018/12/31/2018-28375/privacy-act-of-1974-system-of-records

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Individuals are notified through OCFO-10 SORN, *Financial Systems*, and how they can contact have any information corrected. Individuals would also have the right to decline to provide the information at the point of origin of the information. 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. While this data is in the USDA systems it is protected through security controls.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Since the data in RITA is a reflection of data received from the Treasury department and remains unchanged, anyone wanting to ensure their privacy rights are protected should contact the office or person responsible for the originating system (e.g. TREASURY). Agency Privacy Officers are responsible for protecting the privacy right of the customers and employees affected by the interface. Once the data is in the RITA system an individual has been notified via the OCFO-10 SORN, *Financial Systems*, on how to contact USDA on how to obtain information on the PII on them contained in RITA and how to exercise all rights of consent and to change, delete or correct that data in RITA.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The Treasury Agency Privacy Officer and the USDA Privacy Officer once the PII has entered RITA are responsible for protecting the privacy rights of the customers and employees affected by the interface and notification if PII data has become compromised.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about them.

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

The individual is notified through the OCFO-10 SORN, *Financial Systems*, on how to contact USDA/OCFO to gain access to their information. Also, the USDA has a privacy website that provides information on contacting the USDA Privacy Office (**https://www.usda.gov/home/privacy-policy/privacy-office**)

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

The procedures for correcting inaccurate information are in OCFO-10 SORN, *Financial Systems.* Individuals can contact the USDA and obtain the information and then contact USDA to correct inaccurate or incorrect information.

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

The OCFO-10 SORN, *Financial Systems*, provides the methods for correcting their information.

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

Formal redress is provided in OCFO-10 SORN, *Financial Systems.*

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system 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.

8.2 Will Department contractors have access to the system?

The USDA has a limited number of contractors that have access to the RITA developmental effort for this project. Department contractors have access to the system with authorized approval. After completion of proper background investigation, security education and awareness training, contractors are granted access based on job function and the need-to-know principle.

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

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.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Security Assessment and Accreditation for RITA was completed in FY2016. Fiscal year annual testing was conducted for FY17 and FY18 during 2018. FY19 will be the year RITA is re-accredited in accordance with USDA Risk Management Framework Process.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

An audit log is maintained on RITA to effectively trace actions affecting the security of the system to the responsible individual. The log is protected from unauthorized modification, destruction, and access by the limiting access rights to audit logs. A transaction log is maintained using Oracle capabilities that monitor insert, update and delete statements for selected tables. The auditing information captured includes: user ID, object accessed, operation performed, selected before and after images for updates, and the date/timestamp of the transaction. The audit logs are reviewed weekly for instances of possible abuse.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Collected information is related to IPAC intra-governmental funds transfers. Treasury IPAC bulk file transactions may include corporate and individual TINs and SSNs (PII). These PII are provided by Treasury to aid in identifying the origin and purpose of an intra-governmental funds transfer. Authorized USDA personnel may subsequently use this information to associate IPAC intra-governmental funds transfers and amounts with authorized expenditures, and to contact corporate and individual representatives when questions arise.

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

These risks are mitigated by applying the following controls:

- 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.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

RITA is a major mission supportive application. RITA is a web-based database management system that integrates fiscal activity for interagency billings from both Treasury and USDA agencies. These data are reconciled to one another, with unreconciled data identified and assigned to USDA technicians for research and resolution. RITA aids technicians and agency personnel in reconciling agency and Treasury data with a variety of management tools and reports.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

RITA does not employ any technology of concern (e.g., collaborative computing devices, file sharing, etc.).

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

The System Owner and the ISSPM have reviewed and understand OMB memorandums M-10-22 and M-10-23.

10.2 What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

RITA does not utilize third-party websites. However, data is received from manual inputs from online federal agencies and other NFC systems. Customers can then query and print required reports to support the USDA OCFO-FMS mission.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

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

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

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

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

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

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

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

If so, is it done automatically?

Not Applicable.

If so, is it done on a recurring basis?

Not Applicable.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

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

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

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

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

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

10.10 Does the system use web measurement and customization technology?

Not applicable. RITA does not utilize web measurement and customization technology.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of of all uses of web measurement and customization technology?

Not applicable. RITA does not utilize web measurement and customization technology.

10.12 <u>Privacy Impact Analysis</u>: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

. Not applicable. RITA does not utilize web measurement and customization technology

Agency Responsible Officials

ALZAITER CASH-DAVIS Digitally signed by ALZAITER CASH-DAVIS
Date: 2019.07.22 13:16:04 -05'00'

Linda Connolly Date
Office of the Chief Financial Officer
Financial Management Services
Director of TISD
United States Department of Agriculture

KENNETH MCDUFFIE Digitally signed by KENNETH MCDUFFIE
Date: 2019.07.22 13:50:54 -05'00'

Kenneth McDuffie Date
Office of the Chief Financial Officer
Financial Management Services – ISSPM
Director of SSCD
United States Department of Agriculture

Agency Approval Signature

RONALD GROS Digitally signed by RONALD GROS
Date: 2019.07.23 17:02:19 -05'00'

Stanley McMichael Date
Information System
Office of the Chief Financial Officer
Associate Chief Financial Officer/Shared Services
United States Department of Agriculture