USDA Privacy Impact Assessment

Fiscal Year 2024

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed "Gender" and "Sexual Orientation" from Biographical Information in accordance with Executive Order 14168, "Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government."

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Financial Reporting and Improvements and Optimization (FRIO)
Program Office	Office of Chief Financial Officer (OCFO)
Mission Area	Food Safety and Inspection Service (FSIS)
CSAM Number	2474
Date Submitted for Review	

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Keith Komosinski	keith.komosinski@usda.gov	202-937-4212
Information System Security Manager	Marvin Lykes	Marvin.lykes@usda.gov	202-515-6115
System/Program Managers	Martina Simms	Martin.simms@usda.gov	202-937-4201

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 Financial Reporting Improvements and Optimization (FRIO) system is a centralized, data-driven platform designed to enhance financial transparency, accountability, and operational efficiency within the USDA’s Food Safety and Inspection Service (FSIS). FRIO supports critical financial functions—including budget allocation, forecasting, what-if analysis, and execution monitoring—across all FSIS program areas. By consolidating financial data and reporting tools into a single system, FRIO enables more accurate planning, informed decision-making, and real-time oversight of resource use. In addition, robust administrative features such as user and organizational management help streamline internal processes and ensure secure, role-based access. FRIO modernizes financial operations and supports data-informed governance for FSIS

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.

FRIO is owned and managed by FSIS. The system is housed in the Microsoft Datacenter located in Boydton, Virginia. FRIO is integrated into Microsoft Azure and Midrange networks and is not available to the general public or used by a non-Federal entity; it is only available to those with an e-Authentication (e-Auth) username and password logged into the FSIS Enterprise Network. FRIO is not located in a harsh environment that would be detrimental to the hardware or to the system’s performance and availability.

There are several account types in FRIO:

- Administrator
- Budget Analyst
- Budget Execution Branch Chief
- Director
- Financial Management Division (FMD)
- Formulation Administrator
- Formulation Analyst
- Program Manager
- Resource Analyst

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?

The authorities for USDA to collect, maintain, use and disseminate information through this system are: Government Paperwork Elimination Act (GPEA, Pub. L. 105–277) of 1998; Freedom to E-File Act (Pub. L. 106–222) of 2000; Electronic Signatures in Global and National Commerce Act (E–SIGN, Pub. L. 106–229) of 2000; eGovernment Act of 2002 (H.R. 2458/Pub. L. 107– 347); GRAMM-LEACH-BLILEY ACT (Pub L. 106–102).

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

Yes, approved 8/2/2024.

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

USDA/OCIO–2 eAuthentication Service

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

[List additional information collected but not listed above here (for example, a personal phone number that is used as a business number).]

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

The source of the information is the FRIO user.

2.2.1. How is the information collected?

The information collected is provided by the FRIO user to the FRIO administrator.

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

N/A

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

The user providing the information is responsible for providing information accuracy. The user can check FRIO at any time to verify information accuracy on their "My Information" page.

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?

N/A

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

N/A

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?

User information on "My Information" page is used for access to the FRIO application only.

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.

N/A

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?

FRIO users are presented with a Privacy Consent banner that they must acknowledge to gain access to FRIO. Non-consenting will prevent access to FRIO.

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

FRIO users are presented with a Privacy Consent banner that they must acknowledge to gain access to FRIO.

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?

Contact information is retained if the user has access to the system. Access must be a requirement based on user position and status as an employee with FSIS. In FRIO, no accounts are deleted; they are marked inactive. The employee's work phone number and e-mail remain. The business email and business phone numbers are the only PII left in the system.

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.

FSIS has an overarching data retention policy that has been approved by NARA. Please see FSIS Directive 2620.1, Records Management Program.

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.

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.

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 information is not shared.

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

Follow the format below:

Privacy Risk: Not applicable

Mitigation: FRIO does not share PII with other systems or organizations.

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?

Information is not shared externally outside of the USDA.

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 with FRIO access can update their contact information at any time by working with the administrator and giving them the information they need changed, and the administrator will update the "My Information" page. The employee can see it and if incorrectly updated, continue working with the administrator until it is correct.

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

Individuals with FRIO access can update their contact information at any time by working with the administrator and giving them the information they need changed, and the administrator will update the "My Information" page. The employee can see it and if incorrectly updated, continue working with the administrator until it is correct.

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

7.4. Individuals with FRIO access can update their contact information at any time by working with the administrator and giving them the information they need changed, and the administrator will update the "My Information" page. The employee can see it and if incorrectly updated, continue working with the administrator until it is correct.

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

Formal redress is provided in 7.2 above.

7.6. **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.

Mitigation: By 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?

The information is encrypted both at rest and in transit. Data at rest is protected by MS SQL Transparent Database Encryption (TDE). Data in transit is protected by utilizing port 443 and TLS 1.2.In compliance with FIPS 201, "Personal Identity Verification (PIV)", FRIO users must utilize multi-factor authentication (something they know and something they possess) via PIV to authenticate to the FRIO system. The FRIO system security implementation comes from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev.5, "Security and Privacy Controls for Federal Information Systems and Organizations" and Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems".

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

Users must first obtain supervisory approvals. Users must have e-Auth access and must be approved for access to FRIO by the FRIO team in FSIS' Office of the Chief Financial Officer. This is included in system procedures for FRIO.

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

FRIO does not share information.

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

Users are required to undergo Computer Security Awareness Training annually as a condition of continued access to the FSIS systems. In addition, FRIO is used by employees who hold positions of responsibility and are required in their jobs to handle sensitive and confidential information. USDA also has a PII course on AgLearn, "Personally Identifiable Information (PII) Training Course".

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 6/9/2025

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

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.06.26 01:17:17 -04'00'

Signed:_____

Signature of Responsible Officials

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

Signed:_____

Martina Simms
System Owner
FSIS-OCFO
U.S. Department of Agriculture

Signed:_____

Keith Komosinski
Mission Area Privacy Officer
FSIS-OCIO
U.S. Department of Agriculture

Signed:_____

Marvin Lykes
CISO/ACISO
FSIS-OCIO
U.S. Department of Agriculture