Privacy Impact Assessment

Financial Reporting and Improvements and Optimization (FRIO)

- Version: 1.0
- Date: June 30, 2023
- Prepared for: Food Safety and Inspection Service (FSIS)

United States Department of Agriculture

Privacy Impact Assessment for the

Financial Reporting and Improvements and Optimization (FRIO)

June 30, 2023

Contact Point
Martina Simms
Food Safety and Inspection Service (FSIS)
Office of Chief Financial Officer (OCFO)
202-720-3614

Reviewing Official
Timothy Poe
Privacy Office
(202) 205-3828

United States Department of Agriculture

Revision History

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	06/30/2023	Robin Wagner	Creation of new document

Abstract

Financial Reporting Improvements and Optimization (FRIO) eliminates all the manual data manipulation and download efforts by obtaining and organizing data from the source system for easy management and reporting. In the FRIO application, roles and permissions are set so users can selectively access application features and data. In addition, FRIO helps to reduce manual errors and provide reliable and efficient reporting.

FRIO is a centralized reporting and data management application for the financial data of Food Safety and Inspection Service (FSIS) Agency of the United States Department of Agriculture (USDA). FRIO supports budget allocation, forecasting, what-if analysis, and execution monitoring for all FSIS program areas. The system also features a multitude of administrative features, like user management, and organization management.
FRIO is not used by the public or non-Federal entity.
FRIO also uses bot technology, which is a service provided by DISC, using Robotics Process Automation (RPA). The bot is running on an FSIS server hosted on DISC PaaS. The connection is hosting a Windows Virtual Machine (VM), which is used to open a browser allowing the bot to perform multiple functions for FRIO.

Overview

- FRIO is owned and managed by FSIS. The system is housed at the Digital Infrastructure Services Center (DISC) located in Kansas City, MO.
- FRIO is integrated into DISC Enterprise Cloud Platform (ECP) 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.

- The legal authority for the ATO is the OMB Circular No. A-130, *Management of Federal Information Resources, Appendix 1, Federal Agency Responsibilities for Maintaining Records About Individuals; and Authorization to Operate (ATO)*.
- The last FRIO ATO letter is dated 07/30/2020.

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?

FRIO collects the employee's full name, work phone, cell phone, and work e-mail. This information is required input into My Information page to be able to work on FRIO, but is not used in any of the areas within the application.

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

The source of the information within Section 1.1 above, is from the FRIO user. As a mandatory requirement of working on FRIO, the user must supply their information to the application system administrator (SA) for the My Information page.

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

The contact information is collected so the user can work within their role on the FRIO application.

1.4 How is the information collected?

The information shown in Section 1.1 above, is collected by the FRIO user. As a mandatory requirement of working on FRIO, the user must submit their information to the SA to create the My Information page for the user of the application.

1.5 How will the information be checked for accuracy?

FSIS users are responsible for the accuracy of the information they submit to the SA to enter for the My Information page.

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

The authorities for USDA to collect, maintain, use and disseminate information through this system are: 5 U.S.C.301 (government organization and employees); Title 5 USC 552a (Records Maintained on Individuals (Privacy Act)); Title 41 CFR 201-6.1 (Federal Information Resources Management Regulation); 44 U.S.C.3101 (Records Management); OMB Circular No. A-108 (Responsibilities for the Maintenance of Records About Individuals by Federal Agencies); OMB Circular No. A-130 (Management of Federal Information Resources, Appendix 1, Federal Agency

Responsibilities for Maintaining Records About Individuals); and Authorization to Operate (ATO), dated 22-07-14.

In addition, USDA is generally authorized to collect information to support its mission under: Title 7, Chapter 55-2205 (7 U.S.C 2204) (which authorizes the Secretary of Agriculture to collect information and employ any sampling or other statistical method deemed appropriate); 21 U.S.C. 679c(a)(1)-(3) (which expressly authorizes the Secretary to give high priority to enhancing the ability of FSIS to conduct its mission); the Federal Meat Inspection Act (FMIA) (21 U.S.C. 601, et seq.), the Poultry Product Inspection Act (PPIA) (21 U.S.C., et seq.), the Egg Products Inspection Act (EPIA) (21 U.S.C. 1031, et seq.), and the Humane Methods of Livestock Slaughter Act of 1978 (7 U.S.C. 1901-1906).

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

Access to data is strictly controlled, with access granted through the USDA-approved secure single sign-on application (eAuth – Level 2 Access) and authorization within FRIO. Data is encrypted within FRIO utilizing TLS1.2, ECDHE_RSA with P-256 and AES_128_GCM. Cipher specifications in Web/Apache/DIT are all FIPS compliant. Additionally, FRIO is role-based to ensure least privileges.

FRIO System Administrators and general users access the system using unique, authorized accounts. FRIO cannot be accessed without an authorized account, and it cannot be accessed by external users. There are no anonymous user accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

There are firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. The complete set of security controls are tested every three years or when significant modifications are made to the system. Additionally, the USDA has established continuous monitoring, and 1/3 of the controls are now tested as part of the Annual Assessment on the two off years, and the last 1/3 are tested in the third ATO year.

Active Directory and FRIO role-based security are used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system. When anyone is requesting access to the FSIS environment, they are issued a USDA e-mail account and an FSIS user account (managed in Active Directory), before being provided access to FRIO. As noted above, they also will be required to obtain a USDA eAuth Level 2 account to access FRIO. To access FRIO, the user must first login to the FSIS network environment by using their Active Directory account to login. As a

result, their secure network login credentials from Active Directory are checked against authorized system user role membership, and access privileges are restricted accordingly.

The USDA e-Auth is used to login to FRIO. When a user accesses FRIO, there are FRIO-specific user roles that are used to further restrict a user's access. FSIS system users must pass a Government National Agency Check with Inquiries (NACI) background check prior to having system access. Regular, recurring security training is practiced and conducted through the Office of the Chief Information Officer.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Any contractors who may be authorized to access the system (e.g., SW developers) are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel who are experts in such matters.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

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

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

There are no tools used to analyze the data in FRIO

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

FRIO does not use 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.

Access to data is strictly controlled, with access granted through the USDA-approved secure single sign-on application (eAuth – Level 2 Access) and authorization within FRIO. FRIO is role-based to ensure least privileges.

FRIO SAs and general users access the system using unique, authorized accounts. FRIO cannot be accessed without an authorized account, and it cannot be accessed by external users. There are no anonymous user accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

There are firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. The complete set of security controls are tested every three years or when significant modifications are made to the system. Additionally, the USDA has established continuous monitoring, and 1/3 of the controls are now tested as part of the Annual Assessment on the two off years, and the last 1/3 are tested in the third ATO year.

Active Directory and FRIO role-based security are used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the

system. When anyone is requesting access to the FSIS environment, they are issued a USDA e-mail account and an FSIS user account (managed in Active Directory), before being provided access to FRIO. As noted above, they also have to obtain a USDA eAuth Level 2 account to access FRIO. To access FRIO, the user must first login to the FSIS network environment by using their Active Directory account to login. As a result, their secure network login credentials from Active Directory are checked against authorized system user role membership, and access privileges are restricted accordingly.

The USDA e-Auth is used to login to FRIO. When a user accesses FRIO, there are FRIO-specific user roles that are used to further restrict a user's access. FSIS system users must pass a Government National Agency Check with Inquiries (NACI) background check prior to having system access. Regular, recurring security training is practiced and conducted through the Office of the Chief Information Officer.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Any contractors who may be authorized to access the system (e.g., SW developers) are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel who are experts in such matters.

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?

Contact information is retained if the user has access to the system. Access must be warranted 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 phone number is the only PII left in the system.

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

Yes, DAA-0584-2015-003 Request for Records Disposition Authority was approved. FSIS also has an overarching data retention policy that has been approved by NARA. Please see FSIS Directive 2620.1, *Records Management Program*.

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

The length of time data is retained does not affect the type or level of risk. The controls outlined in Section 1.7 provide ongoing privacy protection to the data.

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?

Information is not shared with organizations external to the USDA.

4.2 How is the information transmitted or disclosed?

PII data is not used for reporting or retrieval purposes; therefore is not disclosed.

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.

To have a FRIO account, the user must enter their contact information including first and last name, personal cell phone, FSIS desk phone, and FSIS e-mail addresses. Therefore, the risk is low that a user might share their personal contact data with another user, or with someone who does not have authority to have that information.

FRIO users are routinely provided privacy reminders and take part in annual security awareness training to mitigate that risk.

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?

Information is not shared with organizations external to 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.

FRIO does not share PII outside of the Department.

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

The United States does not have a single overarching data protection law beyond the provisions of HIPAA and other legislation pertaining to healthcare.

Therefore, *should* FRIO information ever need to be shared externally, FRIO would follow all industry-specific guidelines and requirements for providing information to external organizations.

The following are a list of those industry-specific guidelines and requirements:

- *Federal Information Security Management Act (FISMA)*
- *North American Electric Reliability Corp. (NERC) standards*
- *Title 21 of the Code of Federal Regulations (21 CFR Part 11) Electronic Records*
- *Health Insurance Portability and Accountability Act (HIPAA)*
- *The Health Information Technology for Economic and Clinical Health Act (HITECH)*
- *Patient Safety and Quality Improvement Act (PSQIA, Patient Safety Rule)*
- H.R. 2868: *The Chemical Facility Anti-Terrorism Standards Regulation*.

This includes the redacting of PII, unless the information is required under law.

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

If employee PII data is transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee PII is not shared externally. Such information would only be provided if required by law. Standard FSIS or USDA guidelines for protecting the information would be followed.

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 Does this system require a SORN and if so, please provide SORN name and URL.

FRIO does not require a SORN.

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

Yes. Notice is provided to the individual prior to collection of any information, in accordance with USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII) for all Source System users.

The user is told prior to system access that entering their name is a requirement of working on the system; therefore, the user is notified.

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

No. Because collection of the information is a requirement to access FRIO, if they decline, they cannot work on the FRIO system.

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

No.

6.5 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 user is told prior to system access that entering their name is a requirement of working on the system; therefore, the user is notified.

As users submit the data to the application SA and see the data in the system, there is no lack of awareness, and thus, no risk.

Failure to have this information can lead to greater risks in FSIS being unable to respond to an incident.

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?

Individuals with FRIO can update their contact information at any time by working with the application SA and giving them the information they need changed, and the SA will updated on the My Information page. Once there, the employee can see it and if incorrectly updated, continue working with the SA, until it is correct. Additionally, individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA office.

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 2166, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 720-2109 - Fax (202) 690-3023 – E-mail: fsis.foia@usda.gov.

For more information about how to make a FOIA request, please see:

http://www.fsis.usda.gov/wps/portal/footer/policies-and-links/freedom-of-information-act/foia-requests

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

Individuals with FRIO access have the ability to update their personal information by working with the application SA to update it on their personal page. Additionally, the individual wishing to correct inaccurate or erroneous information should contact the system owner.

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

Before providing information, the individual is presented with a Privacy Act Notice and an explanation of the Notice, on both the USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII).

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

N/A. Formal redress is provided. See 7.2 above.

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

The risk is that a user might share personal contact data of another user with someone who does not have authority to have that information. FRIO users are routinely provided privacy reminders and take part in annual security awareness training to mitigate that risk.

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 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.

8.2 Will Department contractors have access to the system?

Yes. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel experts in such matters.

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

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.

8.4 Has Assessment & Authorization been completed for the system or systems supporting the program?

Yes. The Authority to Operate (ATO) was granted on 07/30/2020. This is an ATO year for FRIO.

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

Updates are controlled in that most users are responsible for ensuring their own information is correct, and if not, work through the application SA to update it, or make any changes needed. Only those in executive assistant roles can update their supervisors' information.

FRIO also has activity audit capabilities using two separate reports.

FRIO has the following technical safeguards are in place:

- Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- FIPS 201, *Personal Identity Verification (PIV)*

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*
- Cybersecurity and Infrastructure Security Agency (CISA) *High Value Asset Control Overlay, Version 2.0, dated January 2021*.

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?

The controls noted in 1.7, including eAuth and limited FRIO access, address the general risks. The remaining risk is that a user will share information with someone who is not authorized to have that information. However, the system is used by those in positions of responsibility who are used to handling sensitive and confidential data. This greatly mitigates this risk.

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?

FRIO is a major application.

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

No.

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"?

Yes. Both M-10-22 and M-10-23 have been reviewed by the SO and ISSPM.

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

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

If so, is it done automatically?

N/A - Third party websites are not being used.

If so, is it done on a recurring basis?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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)?

N/A - Third party websites are not being used.

10.10 Does the system use web measurement and customization technology?

No.

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

N/A.

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

N/A.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A.

10.12 Privacy Impact Analysis: 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.

N/A - Third party websites are not being used.

Responsible Officials

Martina Simms
System Owner (SO)
1400 Independence Ave, SW
Washington, DC 20250

Marvin Lykes
Chief Information Security Officer (CISO)
1400 Independence Ave., SW
Washington, DC 20250

Carl A. Mayes
Assistant Chief Information Officer (ACIO)
1400 Independence Ave., SW
Washington, DC 20250

Timothy Poe
Privacy Officer
1400 Independence Ave., SW
Washington, DC 20250

Approval Signatures

Martina System Owner	DATE
Marvin Lykes Chief Information Security Officer (CISO)	DATE
Carl A. Mayes Assistant Chief Information Officer	DATE
Timothy Poe Privacy Officer	DATE