U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

Privacy Impact Assessment

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.

Privacy Impact Assessment

Privacy Impact Assessment for the USDA IT System/Project:

FNCS Salesforce | Integrated Food Management System (IFMS)

Food, Nutrition, and Consumer Service

Date PIA submitted for review:
6/17/2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Deea Coleman	Deea.Coleman@usda.gov	unlisted
Information System Security Manager	John Rosselot Chief, Risk Management Branch	John.Rosselot@usda.gov	571-563-5260
Project Manager, IFMS	Katie Clifford	Katie.Clifford@usda.gov	703-305-7496

Privacy Impact Assessment

Abstract

Integrated Food Management System (IFMS) is built upon the USDA Salesforce GovCloud Plus platform, which is FedRAMP authorized. IFMS enables Food Distribution Program on Indian Reservations (FDPIR) participating Indian Tribal Organizations (ITOs) or State agencies to maintain household certification data, issue USDA foods to certified households, and maintain inventory. This Privacy Impact Assessment (PIA) is required as there are certain personally identifiable information (PII) data elements included in the information collected from those participating in FDPIR.

Overview

The Integrated Food Management System (IFMS) is a software as a service (SaaS) solution that consolidates overall business transactions into a software platform for Food Distribution Program on Indian Reservations (FDPIR) administrating agencies IFMS utilizes the Salesforce Service Cloud web interface. The Rootscan mobile application connects to the Salesforce Service Cloud and synchronizes with the web channel. IFMS utilizes Rootstock, a Salesforce managed package that extends the out-of-the-box capabilities of Salesforce without crossing Salesforce's secure GovCloud authorization boundary. Rootstock provides Enterprise Resource Planning (ERP) modules that allows IFMS users to manage inventory and issue USDA Foods to FDPIR households.

IFMS' household certification module stores household data and makes eligibility determinations per FDPIR certification regulations and policies. Personally Identifiable Information (PII) stored in the system includes household information, individual information, Tribe affiliation, and preference on food pickup locations. This data is provided via registration to the FDPIR program. The data is used to ensure the correct amount of USDA foods is being offered to each household and help ensure that USDA Foods are only distributed to household members and/or their authorized representative.

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 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?

FDPIR is authorized under Section 4(b) of the Food and Nutrition Act of 2008 (codified in the Agriculture Improvement Act of 2018) and Section 4(a) of the Agriculture and Consumer Protection Act of 1973. FDPIR is authorized through 2026. Federal regulations governing the program can be found at 7 CFR Parts 250, 253, and 254.

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

Yes. IFMS is authorized as part of the FNS Salesforce boundary. The most recent authorization was granted on 11/20/2023 and expires on 11/20/2026.

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

Currently the SORN for IFMS is under development.

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

No.

Section 2.0 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?

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)

Privacy Impact Assessment

Identifying Numbers			
☐	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	☐	Sexual Orientation	☐	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

Identifying Numbers					
☐	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

In addition, IFMS collects the following PII that is not identified on the table above:

- Household ID
- Household Size
- Household Status
- _____Tribe

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

IFMS receives this information directly from the individual applying for the FPDIR program.

2.2.1. How is the information collected?

Information is provided during the FDPIR application process.

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.

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

FDPIR Certifier Roles (Certifier and Approver) are responsible for verifying and correcting PII used for FDPIR certification and then entering the information in IFMS.

7 CFR 253.5(i) requires that the FDPIR review program operations at least annually; this includes the review of household certification information. Any deficiencies must be documented, and corrective action must take place. Additionally, FDPIRs are subject to the auditing requirements per 2 CFR 200, Subpart F.

FNS also conducts FDPIR Management Evaluations, and part of this review includes a review of the casefile records. Any deficiencies are provided via a report that includes corrective action. The FDPIR must address each corrective action and provide validation that said corrective action has taken place.

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?

Not Applicable

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

Not Applicable

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

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.

Mitigation: Addressing risks through proper data characterization practices is essential for maintaining compliance with the PA and protecting individuals' personal information. Implementing the following mitigation actions, mission areas 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.

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?

IFMS receives and processes data on participants of the FDPIR program. This PII includes household information, individual information, and Tribe affiliation. This data is provided via registration to the FDPIR program.

The data is used to ensure the correct amount of USDA foods is being offered to each household and to verify the identity of the household member picking up the food.

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.

Tools used are Salesforce Reports, Salesforce Dashboards, and Tableau. All of these tools can produce reports or graphics that can summarize the data. Reports generated from this data include Household, Household Member, inventory/product, and transaction data.

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

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.

Mitigation: By Implementing some or all the following mitigation actions, mission areas 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.

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 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?

U.S. Government intention to collect PII is stated in the System of Record under development to be published in the Federal Register. With the System of Record Development, Privacy Act Statements or Advisories are also under development for provision to FDPIR partners in order to ensure notification of protections and access rights.

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

Individuals seek benefits voluntarily and are given the opportunity and have the right to decline to provide information.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

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.

Mitigation: Implementing the following mitigation actions, mission areas 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.

User Rights: Inform users about their rights regarding their personal data, including access, correction, deletion, and the ability to object to processing.

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?

IFMS will permanently retain records as defined within the NC1-462-79-02 retention schedule. This includes the database/master file, household data, certification data, inventory data, and outputs and reports (FNS-101 and FNS-152).

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Yes. Approval was provided on October 2, 2024, per the FNS EIS Scheduling Questionnaire for FNS Salesforce IFMS Version 1.0.

5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information.

Privacy Risk: Risk associated with data retention are primarily centered around the increase of exposure to data leaks that is inherit with storing more data than necessary.

Mitigation: Only use NARE approved records schedule proposed for records retention and disposal. Maintenance and destruction timelines mitigate data protection risk and ensure currency of information.

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?

N/A. IFMS does not share PII internally.

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

Privacy Risk: The privacy risks are centered around the unauthorized disclosure of the PII hosted in the Salesforce Government Cloud Plus environment.

Mitigation: Salesforce Government Cloud Plus utilizes Salesforce's Shield Platform Encryption to mitigate the threat to unauthorized disclosure of PII. With Shield Platform Encryption, the System Administrator can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports user accounts, cases, search, approval processes, and other key features. Access to IFMS is also tightly controlled through the use of Login.gov and least role privileges.

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?

None, the IFMS information stays within the system. The system itself is protected by role-based access layers and positive identification and authentication techniques to ensure only people authorized to view and act upon information about others can do so.

FDPIR program administers with limited role-based access can view and edit information in IFMS to facilitate benefits.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Privacy Risk:

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 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 7.0 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 may obtain information regarding the procedures for gaining access to their own records contained within IFMS by contacting FDPIR program administrators or the Freedom of Information Act (FOIA) office.

A request for information should contain the name of the individual, the individual's correspondence address, the name of the system of records, the year of the records in question, and any other pertinent information to help identify the file.

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

Procedures for contesting records are the same as procedures for record access in section 7.1 above. The reason for contesting the record and the proposed amendment to the information should be included along with any supporting documentation that shows how the record is inaccurate, or information is erroneous.

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

Notification procedures will be provided in the System of Records notice under development. Procedures for contesting records are the same as procedures for record access in sections 7.1 and 7.2 above.

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

If formal redress is not possible after contacting USDA in accordance with established procedures, individuals are directed to utilize other legal measures to correct erroneous information, including but not limited to, filing civil and/or criminal complaints.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

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: Implementing the following mitigation actions, mission areas 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.

Timely Response Protocols: Implement protocols for acknowledging and responding to redress requests promptly, ensuring that individuals feel heard and valued.

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?

IFMS, built upon the Salesforce GovCloud Plus platform, utilizes a robust collection of technical safeguards to ensure the integrity of the platform. IFMS is hosted in a secure server environment that uses a firewall to prevent interference or access from outside intruders. When accessing IFMS, Secure Socket Layer (SSL) technology protects the user's information by using both server authentication and data encryption.

IFMS administrators will have a suite of security tools that can be used to increase the security of the system. From a physical security standpoint, the servers that host IFMS are stored in a