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:

FNS Salesforce

Food, Nutrition, and Consumer Service

Date PIA submitted for review:
10/10/2023

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Wilson Moorer Interim FNCS Privacy Officer	Wilson.Moorer@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
Project Manager, FDP, WIMS, Mercury	Khalid Plastikwala	khalid.plastikwala@usda.gov	703-718-1624
Project Manager, SVC	Erin McBride	erin.mcbride@usda.gov	703-305-2709
Project Manager, TODOS	Shobha Jayakumaraswamy	Shobha.Jayakumaraswamy@usda.gov	443-465-3194
Project Manager, SCOUT 2.0	Kathleen McKillen, John Flynn	Kathleen.McKillen@usda.gov John.Flynn@usda.gov	703-967-2030 703-605-0878

Privacy Impact Assessment

Abstract

FNS Salesforce provides the hosting environment for Food, Nutrition, and Consumer Services (FNCS) applications deployed in the United States Department of Agriculture (USDA) Salesforce Government Cloud environment, which is FedRAMP Authorized. The Salesforce Government Cloud is a partitioned instance of Salesforce's Platform-as-a Service (PaaS) and Software-as-a-Service (SaaS), multi-tenant community cloud infrastructure specifically for use by U.S federal, state, and local government customers, U.S. government contractors, and Federally Funded Research and Development Centers (FFRDCs). The Salesforce Government Cloud is comprised of the Salesforce Services: Lightning Platform, Sales, Service, Communities, Analytics, and Industry Solutions. FNS Salesforce is an implementation of Salesforce that hosts multiple applications spanning across multiple functional areas within FNS. The Salesforce platform allows for faster delivery and sharing of information from other applications residing within the same Salesforce Org. Overall, the FNS Salesforce Apps will assist in minimizing the creation of duplicative solutions within the agency and the removal of day-to-day manual processes.

In addition to the USDA Salesforce Government Cloud (GovCloud) environment, the FNS Salesforce authorization boundary also includes an instance of Salesforce GovCloudPlus managed by the Manhattan Strategy Group (MSG).

Overview

Food Delivery Portal (FDP) is owned and operated by USDA FNCS. FDP will host vendor management data submitted by State agencies for the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) and will be critical to providing effective federal oversight of the WIC Program. FDP will contain information on State agency performance regarding vendor training, visits, investigations, violations, sanctions, compliance, monitoring, and redemptions as well as vendor information such as store name, store address, tax identification number, and assigned agency number.

The Integrated Food Management System (IFMS) enables Food Distribution Program on Indian Reservations (FDPIR) participating Indian Tribal Organizations (ITOs) or an agency of a state government to capture household data, track certification periods, issue USDA Foods to certified households, and maintain inventory.

Mercury is a correspondence tool for Supplemental Nutrition Assistance Program (SNAP), SNAS, CNP and Retailer Operations and Compliance (ROC) to receive and process communications from the public or congressional letters, congressional report requests, FNS internal sources, and other correspondence requiring USDA response.

States Systems Comprehensive Outlook & Unified Tracker 2.0 (SCOUT 2.0) is a program management tool used by the USDA State Systems Office (SSO) and program resources to support the USDA FNCS Advance Planning Document (APD) processes. The APD process in which states request and receive prior approval and Federal funding to Buy, build, transfer, license, enhance or modify the systems used by State SNAP and WIC programs to determine

eligibility for participation and to issue benefits. SCOUT 2.0 is built using FNS Salesforce platform and the application has no integration with any other application.

Store Visit Contract (SVC) utilizes the Salesforce GovCloud Plus platform to service the SNAP Retailer Visit Contract. The SVC system receives, processes, and delivers retailer data to include retailer personally identifiable information (PII) to Retail File System (RFS)/Store Tracking and Reporting System (STARS). The data delivered is vital to allow FNCS to make informed decisions regarding retailer eligibility to accept SNAP benefits, continuous re-authorization, and take administrative actions.

Tracking Optimization & Deliverable Oversight System (TODOS) App is a project-management application for contracted research projects.

Waiver Information Management System (WIMS) allow states to submit waiver requests (or modify existing waiver requests) and policy questions through a unified portal. These requests will be automatically routed through FNCS regional offices and the National Office for processing. A privacy impact assessment (PIA) is being conducted because WIMS collects and stores first and last names of users outside of the USDA.

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?

7 CFR § 246.12 is the specific legal authority that defines the collection of information. New System of Records (SOR) Notice (SORN) entitled USDA/FNS-12, Food Delivery Portal (FDP), which is a system used to house state agency vendor management data for the Special Supplemental Nutrition Program (SNAP) for Women, Infants, and Children (WIC), is in routing for approval to/thru the Departmental Privacy Office under the Office of the Chief Information Officer using the Executive Correspondence Management system. This SOR maintains records of activities conducted pursuant to FNCS' mission and responsibilities authorized by legislation.

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 2023. Federal regulations governing the program can be found at 7 CFR Parts 250, 253, and 254.

7 U.S. Code Chapter 51, 2018, Sec. 9.10(a)(1)(D) states no retailer food store or wholesale food concern shall be approved to be authorized or reauthorized for participation in SNAP unless a store visit has been conducted.

USDA Form FNS-674 and FNS-674 Component Addendum and SCOUT 2.0 information collected is required to perform required business function.

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

Yes.

- The Security Plan Status: Approved
- The Security Plan Status Date: 09/19/2023
- The Authorization Status: Approved
- The Authorization Date: 8/21/2023
- The Authorization Termination Date: 8/26/2026
- The Risk Review Completion Date: 12/20/2022
- The FIPS 199 classification of the system: Moderate

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

Yes. SORN USDA/FNS-12, https://www.federalregister.gov/documents/2021/10/07/2021-21941/privacy-act-of-1974-proposed-new-system-of-records. This SOR maintains records of activities conducted pursuant to FNS' mission and responsibilities authorized by legislation. 7 CFR § 246.12 is the specific legal authority that defines the collection of information.

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?

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

Identifying Numbers			
☐	Student ID Number	☐	Federal Student Aid Number
☐	Passport number	☐	Alien Registration Number
☐	DOD ID Number	☐	DOD Benefits Number
☒	Employee Identification Number	☐	Professional License Number
☐	Taxpayer Identification Number	☐	Business Taxpayer Identification Number (sole proprietor)
☐	Credit/Debit Card Number	☐	Business Credit Card Number (sole proprietor)
☒	Vehicle Identification Number	☐	Business Vehicle Identification Number (sole proprietor)
☐	Personal Bank Account Number	☐	Business Bank Account Number (sole proprietor)
☐	Personal Device Identifiers or Serial Numbers	☐	Business device identifiers or serial numbers (sole proprietor)
☒	Personal Mobile Number	☐	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number		

Biographical Information					
☒	Name (including nicknames)	☐	Gender	☐	Business Mailing Address (sole proprietor)
☒	Date of Birth (MM/DD/YY)	☒	Ethnicity	☐	Business Phone or Fax Number (sole

Identifying Numbers					
					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

Identifying Numbers					
☐	Hair Color	☐	Eye Color	☐	Height
☐	Video recording	☐	Photos	☐	Voice/ Audio Recording
☐	DNA Sample or Profile	☐	Signatures	☐	Weight

Medical/Emergency Information					
☐	Medical/Health Information	☐	Mental Health Information	☒	Disability Information
☐	Workers' Compensation Information	☐	Patient ID Number	☐	Emergency Contact Information

Device Information					
☐	Device settings or preferences (e.g., security level, sharing options, ringtones)	☐	Cell tower records (e.g., logs, user location, time, etc.)	☐	Network communications data

Specific Information/File Types					
☐	Personnel Files	☐	Law Enforcement Information	☐	Credit History Information
☐	Health Information	☐	Academic/Professional Background Information	☐	Civil/Criminal History Information/Police Record
☐	Case files	☐	Security Clearance/Background Check	☐	Taxpayer Information/Tax Return Information

Additional data elements collected by one or more FNS Salesforce applications: Tribe, Preferred pickup site, Primary Phone, Secondary Phone, Household Size, Household ID, Store number identifier, Policy data, State agency users, Annual vendor data, Training, Redemptions, Investigations, Violations, Compliance buys, Sanctions, Hours of operation, Store owners, Account history.

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

Information is collected via WIC State agencies, external correspondence (letters and emails) to FNCS, FNS-674 forms and its component addendum, SNAP waiver requests (initial, extensions, or modifications), waiver responses along with accompanying reports, SCOUT 2.0 and information collected directly from the retailer business to include retailer personnel.

New contacts are captured when formal requests for funding comes from State agencies in email or documents that State submits.

2.2.1. How is the information collected?

State agency users can either manually input data into the system or can upload data by using CSV and XML files. The WIC Program also has a data sharing agreement with the SNAP, which imports data between FDP and the STARS systems. Other information is collected from FNS-674 forms. Information is also collected by reviewers performing unannounced visits the retailer locations.

SCOUT 2.0 SSO users will collect information from state directly when funding requests are submitted.

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

FDP utilizes commercial Geographic Information System (GIS) mapping to map the location of vendor stores.

SVC uses commercial information provided by the retailer and FNS through the application to join SNAP.

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

Data that is submitted into the Salesforces apps will be checked for accuracy through validation checks to ensure that the data is accurate before it is saved in the system. FDPIR Certification Administrators are responsible for verifying and correcting PII used for FDPIR certification and then entering the information in IFMS. SVC utilizes a team of Quality Control personnel to compare store visit survey data against photographic support collected at the same time of the visit. SCOUT 2.0 information is received through formal documents or emails from state agencies and SSO Analysts verify the information before entering it into the system.

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?

Third-party websites are not used.

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

Third-party websites are not used.

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

Privacy Risk: The privacy risks associated with FNS Salesforce are centered around the unauthorized disclosure of the PII hosted on the platform.

Mitigation: FNS Salesforce utilizes 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 Salesforce features. Access to FNS Salesforce is also tightly controlled through the use of eAuthentication and least role privileges.

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?

The information is collected so that FNCS can provide effective federal oversite over the WIC Program. The information will be used to inform FNCS on state agency performance regarding vendor training, compliance, monitoring, and sanctions. Additionally, the collection of information verifies that the correct amount of USDA food is being offered to each household, to ensure it is delivered if needed, and to verify the identity of the household member picking up the food. The collection also enables FNCS to answer external correspondence (letters and emails) and track the agency's responses.

SCOUT 2.0 information is collected to have contact information of State contacts involved in the projects being funded.

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. Data produced are waiver metrics and approval/denial of payments.

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

Privacy Risk: The privacy risks related to the use of information are centered around compromising information that is being stored.

Mitigation: USDA safeguards records in this system according to applicable rules and policies, including all applicable USDA automated systems security and access policies. USDA has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

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?

- State Agencies and vendors who choose to participate in the WIC Program are required to submit specific information to FNCS. State agencies and vendors are notified of the program and information collection authorities and prior to participating including Privacy Act Statements when applicable.
- When completing the FNS-674, contractors and partners will sign an acknowledgement of understanding the Privacy Act Statement provided within the document.
- Retailers applying or participating in SNAP are informed that store visits are required. And, prior to beginning the store visit, retailers are given the option to consent to an unannounced visit. Providing consent allows the SVC Reviewer to collect retailer information to include PII.
- U.S. Government intention to collect PII will be 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?

- Vendors and state agencies who choose to participate in the WIC Program do not have the opportunity and/or right to decline to provide required information, nor do they have the right to consent to particular uses of the information.
- Individuals seek benefits voluntarily and are given the opportunity and have the right to decline to provide information.
- For Mercury, individuals cannot decline; the information uses are specific and required in order to be granted access to Mercury within FNS Salesforce.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Privacy Risk: The privacy risks related to notice are focused on the collection of data with from vendors and state agencies without their consent.

Mitigation: Notice is provided to the vendors and state agencies who choose to participate in the WIC Program during their initial onboarding process. There is no risk with the vendors or state agencies being unaware of the requirement for collection of information, as state agencies are responsible for submitting the information they collect on their vendors into FDP.

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?

FDP: FDP does not have currently have a records schedule that is approved by the National Archives and Records Administration (NARA). The proposed schedule dictates that the different information sets will be retained for different periods of time, as described below. The records within FDP will be kept indefinitely until NARA has approved a records schedule for FDP.

FDP's Database/Master file will be retained on a temporary basis and will be destroyed either 10 years after the termination of the system and the successful migration of the data or 10 years after the termination of the system.

The Electronic Food Delivery Portal Data Entry Form, which represents an input to FDP, will be retained in accordance with GRS 5.2, Item 020 on a temporary basis and destroyed upon verification of the successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Outputs and Reports generated by FDP, which will be retained in accordance with GRS 5.2, Item 020, can be in any of the following formats: electronic, metadata, reference data, or paper. Outputs and Reports will be kept on a temporary basis and destroyed upon verification of the successful creation of the final document or file, or when no longer needed for business use, whichever is later.

System Documentation for FDP will be retained in accordance with GRS 3.1, Item 051. System Documentation for FDP includes data system specifications, file specifications, codebooks, record layouts, user guides, output specifications, and final reports (regardless of medium) relating to a master file, database or other electronic records. System Documentation will be retained on a temporary basis and destroyed 5 years after the project/activity/transaction is completed or superseded, or when the associated system is terminated, or when the associated data is migrated to a successor system.

The information in FDP will be retained on the abovementioned schedule to allow FNS to analyze nationwide trends in vendor and contractor data while also providing assurances to Congress, the Office of Inspector General, senior program managers and the general public that every reasonable effort is being made to prevent, detect and eliminate fraud, waste, and abuse. FDP will support FNS in formulating program policies and regulations, generating an annual report to assess state agency progress in assessing the level of activity that is being completed to ensure program integrity, and analyzing trends over a 5-year period.

IFMS: The IFMS database/master file will be retained on a temporary basis for a period of three years from the date of the submission of the annual financial status report, SF-425; except that, if any litigation, claim or audit is started before the expiration of the three year period, the records shall be retained until all litigation, claims or audit findings involving the records have been resolved, in accordance with 7 CFR 253.5

The household, certification, and inventory data, which represents an input to IFMS, will be retained in accordance with GRS 5.2, Item 020 on a temporary basis and destroyed upon verification of the successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Outputs and Reports (FNS-101 and FNS-152) generated by IFMS, which will be retained in accordance with GRS 5.2, Item 020, can be in any of the following formats: electronic, metadata,

reference data, or paper. Outputs and Reports will be kept on a temporary basis and destroyed upon verification of the successful creation of the final document or file.

Mercury: System Access Records/Audit records are disposed of in accordance with NARA: FNS-22 (Controlled Correspondence Files), GRS 5.1-20 (Non-Recordkeeping Copies of Electronic Records listed in the FNS Instruction), and GRS 6.4-20 (Public Correspondence and Communications Not Requiring Formal Action) within the FNS 270-1, Records Management Program - Exhibit A - Records Retention Schedule.

Disposition Authority(s):

- NC1-462-79-2
- DAA-GRS-2016-0016-0002
- DAA-GRS-2016-0005-0002

SCOUT 2.0: SCOUT does not have any archival or deletion planned.

SVC: Salesforce will retain retailer information for a period of 1-year of being confirmed. After one (1) year, Salesforce will transfer the deliverables to an AWS S3 repository for cold storage. The data within AWS S3 can only be accessed and retrieved by authorized Privilege users. After six (6) months, the retailer information is removed from AWS S3 permanently.

TODOS: System Access Records/Audit records are disposed of in accordance with NARA General Records Schedules 3.2, Item 030 listed in the FNS Instruction 270-1, Records Management Program - Exhibit A - Records Retention Schedule.

WIMS: Record retention is covered by NARA approved records retention schedule, Records Schedule Number DAA-0462-2019-0001. See FNS Instruction 270-1, Rev 3 - Exhibit A, Records Retention Schedule for additional details.

Disposition Instructions: Cutoff in the FY when waiver is superseded or obsolete. Destroy 15 year(s) after cutoff.

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: IFMS, TODOS, WIMS, Mercury. All record retention schedules are found in section 5.1.

No: SVC (EIS is in development), SCOUT 2.0 (EIS under review)

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

Privacy Risk: The privacy related 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: The records schedule proposed to NARA represents ideal timelines 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?

Employees and contractors from the Department's FNCS Program Integrity and Monitoring Branch (PIMB) are responsible for conducting federal oversight of the WIC Program and are the primary users of the information. SNAP will be able to access a portion of the data, in order to facilitate review of and reporting on food providers that exist in both programs. Additional programs operated by the Department, within FNCS, may also receive a designated sub-set of data in the future. Information is shared between FNCS Regional and National Office employee/contractors for the purpose of the USDA Digital Service Center (DSC) creating users in FNS Salesforce and for reviewing and responding to waiver requests. Information is also shared with external state agency employee users for waiver requests and responses. SCOUT 2.0 contacts are not shared with any internal organization other than SSO.

Waiver requests and responses are submitted between regional, national, and state agency users.

FNS-674, User Access Request Form and FNS-674 addendum (under development) are transmitted through USDA email for system access. An Internal review process with different tiers of approval exists within FNCS.

Telephone verification process.

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 on the FNS Salesforce platform

Mitigation: FNS Salesforce utilizes 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 FNS Salesforce is also tightly controlled through the use of eAuthentication 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?

Consistent with USDA's information sharing mission, information stored in FNS Salesforce may be shared with other USDA components, as well as appropriate Federal, State, local, tribal,

foreign, or international government agencies. This sharing will only take place after USDA determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions.

PII household data is collected by the Indian Tribal Organization participating in the FDPIR program.

Information sharing with external organizations is limited to USDA partners and contractors with active projects hosted in FNS Salesforce. Information is shared in email and is specific to projects contracted specifically that External Organizations. Project Information may include Project Name, Project Stage, Project Deliverables, Contracting Firm, Project Number, Project Start and End dates, and proposed budget, Project Owner Name, Project Stage, Project Phase, and USDA contact email.

Waiver information may include first and last names of users and email addresses associated with user accounts.

Information is shared outside of the department by email alert message to an external contact. Information shared is limited to name and email address as required to send the email notices. This information may appear on the waiver records as well.

FNCS transmits retailer information via secure web-services that require authorized user credentials to access SF and provide retailer information. Salesforce, in return, will use secure web-services using authorized user credentials to transmit the store visit deliverables. Users requesting access to these user credentials and web-service setup must go through written request and background clearance. A separate login and e-authentication is required to access FNS RFS and STARS.

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

Privacy Risk: The privacy risks are centered around the unauthorized disclosure of the PII hosted on the platform.

Mitigation: FNS Salesforce utilizes 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 Salesforce is also tightly controlled through the use of eAuthentication and least role privileges.

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?

FDP: FDP contains information on WIC vendor management activities, not specific individuals.

IFMS: Individuals may obtain information regarding the procedures for gaining access to their own records contained within IFMS by contacting FDPIR program administrators or the FNCS Privacy Office.

Mercury: Contractors and partners doing business with USDA can contact their contracting officer's representative (COR) or program POC to request access to their FNS-674. They may also submit a Privacy Act Request to the FNS Privacy Officer for access to applicable correspondence information.

SCOUT 2.0: Contractors and partners doing business with USDA can contact their COR or Program POC to request access to their FNS-674 They may also submit a Privacy Act Request to the FNS Privacy Officer for access to applicable correspondence information.

SVC: Retailers do not have access to their information to include PII. Retailers may contact FNS directly via RSC if they would like to request access to their information.

TODOS: Contractors and partners doing business with USDA can contact their contracting officer's representative (COR) or program POC to request access to their FNS-674. They may also submit a Privacy Act Request to the FNS Privacy Officer for access to applicable correspondence information.

WIMS: Contractors and partners doing business with USDA can contact their COR or Program POC.

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

FDP: Contains information on WIC vendor management activities, not specific individuals. State agencies have access to their data and are responsible for correcting any inaccurate or erroneous information that they have submitted into FDP.

IFMS: Individuals may obtain information regarding the procedures for gaining access to their own records contained within IFMS by contacting FDPIR program administrators or the FNS Privacy Office.

Mercury: Contractors and partners doing business with USDA can contact their COR or Program POC. They may also contact the FNS Privacy Officer.

SCOUT 2.0: Contractors and partners doing business with USDA can contact their COR or Program POC. They may also contact the FNS Privacy Officer.

SVC: SVC Reviewers allow retailer personnel to provide retailer information to include retailer PII. The information is collected and securely transmitted from SVC Salesforce to RFS/STARS for FNS review. The retailer may opt to make a correction at the time of the visit where the correct information will be documented. Alternatively, the retailer may contact the retailer call center for further guidance.

TODOS: USDA Users will be contacted through email by COR or Program POC if FNS-674 information or other information needs to be corrected.

WIMS: Contractors and partners doing business with USDA can contact their COR or Program POC.

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

FDP: Contains information on WIC vendor management activities, not specific individuals.

IFMS: 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.

Mercury: USDA Users will be contacted through email by COR or Program POC if FNS-674 information needs to be corrected. Contractors and partners doing business with USDA can contact their COR or Program POC to request updates to incorrect information. They may also receive procedural information from the FNS Privacy Officer.

SCOUT2.0: USDA Users will be contacted through email by COR or Program POC if FNS-674 information needs to be corrected. Contractors and partners doing business with USDA can contact their COR or Program POC to request updates to incorrect information. They may also receive procedural information from the FNS Privacy Officer.

SVC: If the information collected is not correct, the individual has an opportunity to provide the correct information to the SVC Reviewer at the time of the visit. In addition, they may also contact the RSC to address issues they might have.

TODOS: USDA Users will be contacted through email by COR or Program POC if FNS-674 information needs to be corrected. Contractors and partners doing business with USDA can contact their COR or Program POC to request updates to incorrect information. They may also receive procedural information from the FNS Privacy Officer**.**

WIMS: USDA users will be contacted through email by COR or Program POC if FNS-674 information needs to be corrected. Contractors and partners doing business with USDA can contact their COR or Program POC to request updates to incorrect information.

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: The privacy risks are centered around the unauthorized disclosure of the PII hosted on the platform.

Mitigation: Individuals concerned that their PII data may have been compromised may contact the USDA office designated within the System of Records notice posted in the Federal Register.

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?

FNS Salesforce utilizes a robust collection of technical safeguards to ensure the integrity of the platform. FNS Salesforce is hosted in a secure server environment that uses a firewall to prevent interference or access from outside intruders. When accessing FNS Salesforce, Secure Socket Layer (SSL) technology protects the user's information by using both server authentication and data encryption. FNS Salesforce 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 FNS Salesforce are stored in a privately owned data center with strict physical access control procedures in place to prevent unauthorized access.

Access to systems inside of the Salesforce Government Cloud storing U.S. government, U.S. government contractors, and customer data that potentially permit access to customer data are restricted to Qualified U.S. Citizens. Qualified U.S. Citizens are individuals who are United States citizens, are physically located within the United States when accessing the Salesforce Government Cloud systems and have completed a background check as a condition of their employment with Salesforce.

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

USDA safeguards records in this system according to applicable rules and policies, including all applicable USDA automated systems security and access policies. USDA has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

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

Information sharing requirements are reviewed and approved on a yearly basis according to our annual assessment and review schedule.

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

USDA requires all users to complete annual Information Security Awareness training, which includes modules on privacy training.

Privacy Impact Assessment

Approval Signatures:

_____

Joseph Shaw, System Owner
Food, Nutrition, and Consumer Service
United States Department of Agriculture

_____

Wilson Moorer, Interim Privacy Officer
Food, Nutrition and Consumer Service
United States Department of Agriculture

_____

John Rosselot, ISSPM
Food, Nutrition and Consumer Service
United States Department of Agriculture

_____

Chief Privacy Officer
United States Department of Agriculture