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

DATASET, FDP, Mercury, SCOUT 2.0, TODOS, WIMS, and WiSP

Food, Nutrition, and Consumer Service

Date PIA submitted for review:

7/24/2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Deea Coleman FNCS Privacy Officer	Deea.Coleman@usda.gov	unlisted
Information System Security Manager	John Rosselot Chief, Risk Management Branch	John.Rosselotjr@usda.gov	571-563-5260
Project Manager, DATASET	Lenora Hayes	Lenora.Hayes@usda.gov	703-819-6372
Project Manager, FDP, WIMS, Mercury	Khalid Plastikwala	Khalid.Plastikwala@usda.gov	703-718-1624
Project Manager, SCOUT 2.0	Kathleen McKillen,	Kathleen.McKillen@usda.gov	703-967-2030
Project Manager, TODOS	Shobha Jayakumaraswamy	Shobha.Jayakumaraswamy@usda.gov	443-465-3194
Project Manager, WiSP	Laura Stretch	Laura.Stretch@usda.gov	970-413-0321

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).

These applications include Food Delivery Portal (FDP), Data Analysis and Tracking Application for Supplemental Nutrition Assistance Program (SNAP) Employment and Training (DATASET), Waiver Information and State Plans (WiSP), Waiver Information Management System (WIMS), Tracking Optimization & Deliverable Oversight System (TODOS), Mercury, and States Systems Comprehensive Outlook & Unified Tracker 2.0 (SCOUT 2.0). These FNS Salesforce applications utilize certain personally identifiable information (PII) data elements as they facilitate FNCS' avoidance of duplicative solutions within the agency and the removal of day-to-day manual processes. The set of named applications, although distinct from each other in terms of business function, operation, and customers, utilize similar PII elements for similar business purposes within the same Salesforce Org; as such, a single Privacy Impact Assessment (PIA) for the set of applications is required.

Overview

DATASET: Provides FNCS Office of Employment and Training (E&T) Services a platform for standardizing and streamlining the collection of States' E&T State Plans, Program Activity Reports (FNS-583) and Annual Reports. The system optimizes and centralizes the review process for Regional users, providing a place for the approval process, automated notifications of pending tasks, and feedback for State users. For National users, DATASET makes the review process more transparent, giving greater clarity into the status of each State's E&T forms. The system also has analytics and visualizations, which facilitate greater understanding of the implementation and efficacy of E&T programs.

FDP: The Women Infant and Children (WIC) FDP is an application used to compile, analyze, and report on data pertaining to State Agency performance around key WIC vendor management functions, including training, monitoring/investigations, and sanctions. FDP also facilitates annual reporting to FNCS by WIC State Agency that operate retail food operations.

Mercury: A system that allows for the processing and tracking of work packages to document FNCS's responses to incoming correspondence from Congress, the public, or other groups of interest, in alignment with USDA's strategic goal of delivering its programs efficiently, and with the support of the Office of Retailer Operations and Compliance (ROC) Division to eliminate fraud, waste, and abuse. Mercury will also

modernize the correspondence processes and store internal FNCS program office memos, including SNAP; the Child Nutrition (CN) Programs; and the Supplemental Nutrition and Safety (SNAS) Program.

SCOUT 2.0: A program management tool used by the USDA State Systems Office (SSO) and program resources to support FNCS' Advance Planning Document (APD) processes 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.

TODOS: A project management database application for contracted research projects. TODOS helps staff members manage projects efficiently, ensuring each contract generally follows the standard 18-step process, and facilitates the management team oversee the overarching business processes, including workload and resource management.

WIMS: A system to facilitate SNAP Agencies' ability to request Federal approval to temporarily waive requirements of the Food and Nutrition Act of 2008 and/or Federal regulations, allowing State SNAP Agencies to implement alternative procedures in place of Federal requirements, within certain parameters and limitations. WIMS helps State and Federal staff members to manage and monitor the waiver request, review, and response process efficiently, as each waiver request generally follows the same process and steps. WIMS also facilitates workload, resource, and records management.

WiSP: Manages the submission, review and approval of annual WIC, Farmer's Market Nutrition Program (FMNP), and Senior Farmer's Market Nutrition Program (SFMNP) State Plans and related requests for waivers to program regulations. The State Plans outline how each State Agency operates their respective programs. Each Federal program issues waivers in response to needs identified based upon challenges reported and their regulations. State Agencies then request a waiver to be applied to their State Agency. WiSP houses the State Plans, State Agency waiver requests, supporting information and functions including a review and approval by FNCS.

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 for FDP. In addition, System of Records Notice (SORN), *USDA/FNS–12, Food and Nutrition Service (FNS), Women, Infants, and Children (WIC) Food Delivery Portal (FDP)*

7 CFR 2.97 (1) and § 210.3 (a) and USDA Departmental Regulation 3060-01 are the specific legal authority that defines the collection of information for Mercury. In addition, System of Records Notice (SORN), *USDA/FNS–13, Food and Nutrition Service (FNS), Mercury.*

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

Yes. DATASET, FDP, Mercury, SCOUT 2.0, TODOS, WIMS and WiSP are authorized as part of the FNS Salesforce boundary. The most recent authorization was granted on 8/21/2023 and expires 8/26/2026.

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.

SORN USDA/FNS-13, https://www.federalregister.gov/documents/2023/09/18/2023-19829/privacy-act-of-1974-new-system-of-records

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?

WIMS: SNAP waiver requests (initial, extension, or modification), responses, and accompanying reports, along with user first and last names of those involved in the workflow to process a waiver. Potential PII stored in the system is identified as First Name, Last Name and work email of Internal USDA employees (Users), and External USDA partners and contractors (State Agency employees/Contractors). Internal/ External USDA employees PII is used to generate username, enable system login and enable email alerts to Users.

TODOS: Potential PII stored in the system is identified as First Name, Last Name and work email of Internal USDA employees (Users), and External USDA partners and contractors (Contacts) Internal USDA employees PII is used to generate username, enable system login and enable email

alerts to Users. External USDA partners and contractors cannot login to FNS Salesforce, and the PII is used to enable and address email notifications for communications to External Contacts.

SCOUT 2.0: SCOUT 2.0 Stores state agency contacts information such as name, work email address, work phone number, and title.

FDP: Collects information on WIC vendor management activities and vendor data. State agency policy data and Food Delivery Entity (FDE) vendors are the subjects of records in FDP. Specific information maintained on those subjects includes policy data, state agency users, annual vendor data, training, redemptions, investigations, violations, compliance buys, sanctions, hours of operation, store owners and account history. These records are maintained on each State agency and FDE once they decide to participate in the WIC Program and after they leave the WIC Program.

DATASET: Potential PII stored in the system is identified as First Name, Last Name and work email of Internal USDA employees (Users), and External USDA State Agency contacts. Internal USDA employees and External USDA State Agency contacts PII is used to generate username, enable system login and enable email alerts to Users.

Mercury: Potential PII stored in the system is identified as First Name, Last Name and work email of Internal USDA employees (Users), and External USDA partners and contractors (Contacts). The Mercury App will also store the First Name, Last Name, physical address, and/or email of individuals or organizations who correspond with the Agency. The information will only be stored for the purpose of responding to correspondence and tracking those responses for future reference. Internal USDA employees' PII is used to generate username, enable system login and enable email alerts to Users. External USDA partners and contractors cannot login to FNS Salesforce, and the PII is used to enable and address email notifications for communications to External Contacts.

WiSP: WIC, FMNP, and SFMNP State Plans and waiver requests (initial, extension, or modification), responses, and accompanying reports, along with user first and last names of those involved in the workflow to process a waiver. Potential PII stored in the system is identified as First Name, Last Name and work email of Internal USDA employees (Users), and External USDA partners and contractors (State Agency employees/Contractors). Internal/ External USDA employees PII is used to generate username, enable system login and enable email alerts to Users.

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

Privacy Impact Assessment

Identifying Numbers			
☒	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)	☐	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	☐		☐	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					
☐	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

Identifying Numbers					
☐	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

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

- **DATASET:** Internal user information comes from FNS-674 access request forms. External State Agency contact information is from ICAM Shared Services (ICAMSS) eAuthentication response that is received when users first login to the application.
- **FDP:** The vendor management data that will is stored within FDP is submitted by WIC State agencies.
- **Mercury:** Information sources are external (to FNCS) correspondence such as letters and emails, and internal FNS-674 and component addendum system access requests.
- **SCOUT2.0:** New contacts are captured when formal requests for funding comes from State agencies in email or documents that State submits.
- **TODOS: Information sources are the FNS-674 and component addendum access request forms, as well as FNCS projects and contracts.**
- **WIMS:** SNAP waiver requests (initial, extensions, or modifications), waiver responses, and accompanying reports.
- **WiSP:** WIC, FMNP, and SFMNP State Plans (initial & amendments submissions) and waiver requests (initial, extensions), responses, and accompanying reports.

2.2.1. How is the information collected?

- **FDP:** 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 Store Tracking and Reporting System (STARS) systems.
- **WiSP:** FNS-674 data is uploaded by users for central storage, tracing, and access. Contacts are created in the system from project point of contact information. Historical data migrated from waiver authority trackers provided by the PIMB Program and State Plan data received from FNS PartnerWeb.

- **WIMS, TODOS, Mercury, SCOUT 2.0, E&T DATASET:** FNS-674 data is uploaded by users for central storage, tracing, and access. Contacts are created in the system from project point of contact information.

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.
- **DATASET, Mercury, SCOUT 2.0, TODOS, WIMS, and WiSP:** N/A

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

- **FDP:** 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.
- **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.
- **DATASET, Mercury, TODOS, WIMS, and WiSP:** For internal USDA employees, the information comes directly from the approved FNS-674, and there are no other checks for accuracy. For external State Agency contacts, the information comes from eAuth, and they are required to be Level 2 Verified.

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?

- **DATASET:** The users' names and emails are only collected to allow access to the system and to send email notifications.
- **FDP:** 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.
- **Mercury:** To enable FNS to answer external correspondence (letters and emails) and track FNS responses **SCOUT 2.0:** Information is collected to have contact information of State contacts involved in the projects being funded.
- **TODOS:** Project and task management activities and communications.
- **WIMS:** Task management activities and communications for waivers.
- **WiSP:** All WIC, FMNP, and SFMNP State agencies are required to submit annual State Plans or State Plan amendments or request Waivers to their State Plan when necessary, or if applicable. The State Plans outline how each WIC State agency operates WIC, FMNP, and SFMNP for their State agency. Waivers are issued in response to needs identified based upon challenges reported.

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 and Salesforce Dashboards. 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?

- **FDP:** 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.
- **DATASET, Mercury, SCOUT 2.0, TODOS, WIMS, and WiSP:** When completing the FNS-674 contractors and partners will sign an acknowledgement of understanding the Privacy Act Statement provided within the document.

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

- **FDP:** 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.
- **DATASET, Mercury, SCOUT 2.0, TODOS, WIMS, and WiSP:** Individuals cannot decline; the information is required for a user to be granted access to FNS Salesforce applications.

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?

- **DATASET:** No archival or deletion planned yet.
- **FDP** does not have currently have a records schedule that is approved by the National Archives and Records Administration (NARA); a proposed schedule dictates that the different information sets will be retained for different periods of time. The records within FDP will be kept indefinitely until NARA has approved a records schedule. Retaining records on the proposed schedule will allow FNCS 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. Further, FDP will support FNCS 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. The proposed records schedule includes:
    - 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.
- **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) are: NC1-462-79-2, DAA-GRS-2016-0016-0002, and DAA-GRS-2016-0005-0002.

- **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.

- **SCOUT 2.0:** 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.

- **WIMS:** Record retention is covered by NARA approved records retention is , 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.

- **WISP:** 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.

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.

- **Mercury, TODOS, WIMS, and WiSP:** Yes; schedules are found in Section 5.1.

- **DATASET, FDP, and SCOUT 2.0:** No.

    - DATASET has no plans to archive or remove records at this time.

    - FDP records retention schedule is pending NARA approved schedule (see Section 5.1).

    - SCOUT 2.0 EIS is 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?

DATASET: The FNS-674 User Access Request Form 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, as well as for reviewing and responding to waiver requests.

FDP: 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.

In addition, the FNS-674 User Access Request Form 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, as well as for reviewing and responding to waiver requests.

Mercury: The FNS-674 User Access Request Form 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, as well as for reviewing and responding to waiver requests.

SCOUT 2.0: The FNS-674 User Access Request Form 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, as well as for reviewing and responding to waiver requests.

TODOS: The FNS-674 User Access Request Form 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, as well as for reviewing and responding to waiver requests.

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

In addition, the FNS-674 User Access Request Form 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, as well as for reviewing and responding to waiver requests.

WISP: The FNS-674 User Access Request Form 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, as well as for reviewing and responding to waiver requests.

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?

- **DATASET:** State Agency contacts have access to the system but can only view/input form data for their specific state. Email notifications contain information about the status of a form, the state, and the year. Both internal and external users can export data in the form of a PDF.
- **FDP:** 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.
- **Mercury:** Mercury does not share or disclose information externally.
- **SCOUT 2.0:** 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, proposed budget, project owner name, project stage, project phase, and USDA contact email.
- **TODOS:** 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.

- **WIMS:** Information sharing with external organizations is limited to USDA partners and contractors with active user accounts hosted in FNS Salesforce. Information is shared in email and is specific to waivers associated with external organizations.

- **WISP:** The application supports eighty-nine (89) different State agencies with data entry/submissions and with the management of their State Plans. State Plans include questions organized by functional program areas and include State/Federal agreements and other important documentation on each State agency's policies and procedures, which are supported with uploaded documentation. The application allows the creating, editing, and managing of the actual questions, as well as the data provided by each State agency. In unique situations, some waivers can be requested by single State agencies. All State agencies have the option for national waivers.

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 alsosupports 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:** Not applicable. The application contains information on WIC vendor management activities, not specific individuals.

- **DATASET, Mercury, SCOUT 2.0, TODOS, WIMS, and WiSP**: Contractors and partners doing business with USDA can contact their contracting officer's representative (COR) or program point of contact 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.

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

- **FDP:** Not applicable. The application 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.

- **DATASET, Mercury, SCOUT 2.0, TODOS, WIMS, and WiSP**: Contractors and partners doing business with USDA can contact their COR or program point of contact. They may also contact the FNS Privacy Officer.

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

- **FDP:** Not applicable. Contains information on WIC vendor management activities, not specific individuals.
- **DATASET, Mercury, SCOUT 2.0, TODOS, WIMS, and WiSP:** USDA users will be contacted through email by COR or program point of contact if their 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**.**

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: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability. Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

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.