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.

Guidance on how to complete the following PIA Questionnaire is found in the USDA PIA Guide.

FNCS Instruction: Before submitting, please ensure all text that was entered in the placeholders matches the normal font for this document. Please do not submit documents with *<<purple italics font.>>*

Privacy Impact Assessment

Privacy Impact Assessment for the USDA IT System/Project:

FNS National Accuracy Clearinghouse (NAC)

Food, Nutrition, and Consumer Service (FNCS)

Date PIA submitted for review:

1/12/2024

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, Jr. Chief, Risk Management Branch	John.Rosselot@usda.gov	571-563-5260
System/Program Managers	Veronica Brown	Veronica.Brown@usda.gov	703-605-0825

Privacy Impact Assessment

Abstract

The system is the FNS National Accuracy Clearinghouse (FNS NAC).

The FNS NAC is a federal system of records that matches information on Supplemental Nutrition Assistance Program (SNAP) participants and applicants submitted, usually daily, by all 53 State agencies that administer SNAP (the 50 States, the District of Columbia, Guam, and the U.S. Virgin Islands). The FNS NAC allows States a quick and efficient way to determine if a person is participating in SNAP in another state. States use this information to take appropriate action to prevent or end duplicate participation.

USDA Food, Nutrition and Consumer Service (FNCS) is providing this Privacy Impact Assessment (PIA) due to the Privacy Threshold Assessment (PTA) determination that the FNS NAC collects personally identifiable information (PII) and is subject to a PIA.

Overview

FNS National Accuracy Clearinghouse (FNS NAC) is owned by the Food, Nutrition and Consumer Service (FNCS). It is hosted by and operates on Microsoft Azure US Government Cloud.

The purpose of the FNS NAC is to enhance program integrity and reduce payment errors in SNAP by providing a secure method for State agencies to match current participant information with each other to prevent and detect duplicate participation.

Each State agency provides PII on current SNAP participants and applicants to FNS NAC including name, date of birth (DOB), social security number (SSN). This information is de-identified by converting to a secure hash before the information is shared to the FNS NAC.

State agencies conduct matches against the FNS NAC to determine if someone is already receiving SNAP benefits in any other State as part of the process of determining an individual’s eligibility for SNAP at application and recertification or when a new household member is being added to an existing case. The FNS NAC also compares SNAP participant information provided by State agencies to detect existing duplicate participation and notifies State agencies when such matches are found.

The FNS NAC also contains case information on current SNAP participants and applicants, like recent benefit issuance dates, participant ID, case ID, case closure date, and vulnerable individual flag (if applicable).

With respect to any information sharing conducted by the program or system:

- The data in the FNS NAC shall only be used for the purpose of preventing duplicate participation in SNAP and shall only be disclosed to persons directly connected with the administration or enforcement of the provisions of the Food and Nutrition Act or SNAP regulations. Access to the FNS NAC is limited to those FNCS or State agency team members (or their authorized contractors) who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions. The use of defined user roles limits the access of authorized users to only the information they need for their job duties.

Below is a general description of the modules and subsystems, where relevant, and their functions.

- Bulk Upload Application Processing Interface (API): Verifies the identity of any system uploading data to the FNS NACS to ensure that only authorized state agency systems can upload participants. Provides mechanisms for each state to provide current enrollment information to the FNS NAC.
- Extract-Transform-Load Module: Processes state uploads provided via the Bulk Upload API. Validates the information shared by each state and transforms it into a standard format. Purges records on individuals once their enrollment is no longer current.
- State Participants databases (one for each state): Stores information to uniquely identify active SNAP enrollees in the state.
- Orchestrator API (Duplicate Participation API): Verifies the identity of any system querying the FNS NAC to ensure that only authorized state agency systems can verify SNAP enrollment; accepts requests from a state to query the FNS NAC for one or more individuals; accepts de-identified PII (i.e., secure hash of name, date of birth, SSN) for each person whose prior enrollment is in question; queries the internal state participant databases to see if the individuals are already enrolled in SNAP; returns every match for every state and contact information at the appropriate state agency, if there are any matches, or indicates that the individuals are not already enrolled. States with matches are notified via emails by the Notification App.
- Query Tool & Collaboration App: Provides a way for authorized members of state agencies to query the FNS NAC via a web interface. Users can provide identifying information for an individual and learn whether that person is already enrolled for SNAP in another state. Plain text PII is accepted (i.e., name, date of birth, SSN) and immediately de-identified on the client (state agency) side prior to submission to the Orchestrator API.
- Collaboration API (Match Resolution API): Verifies the identity of any system making requests to the FNS NAC to ensure that only authorized state agency systems can retrieve match information and resolve matches; accepts requests from a state to query the FNS NAC for a match or update details for a match as States work to resolve them; accepts a unique match ID and match metadata; queries the internal collaboration database to see if the match exists; updates match with desired information; returns match if it exists;
- Collaboration Database: Stores match information and information about all steps States have taken to resolve matches. Resolution steps taken by States are communicated to matching States via emails by the Notification App.

- Metrics Collector: Gathers information on system operations and stores them in the metrics database. This includes aggregated information like total number of queries and number of positive matches in each state but does not include PII.
- Metrics Database: Stores aggregated information about system performance. Does not store PII.
- Metrics API: Provides a way for FNCS systems (specifically, the FNCS dashboard) to report on the usage and performance of the FNS NAC.
- State Metadata API: This is utilized by the FNS NAC internally; it is not exposed outside of MS Azure. This API keeps track of state metadata, (e.g., email, phone number, region).
- Dashboard App: Provides information to FNCS staff that can be used to measure success of the FNS NAC and identify likely paths to improve it. This may include false positives, return on investment estimates, and common causes for duplicate participation.
- Notification App: Connects to the email service provided by FNCS to send simple email notifications to States for matches and match resolution updates. The emails sent to States contain no PII.
- Match Lookup Database: Stores dictionary of lds_hash and state information, used for performant identification of duplicate participation.
- Maintenance App: Provides static page to users, informing them that the FNS NAC is temporarily undergoing maintenance.
- Developer Portal: Provides secure content management system for sharing FNS NAC documentation and information with State agencies.
- Support Tools API: This is utilized by the FNS NAC internally; it is not exposed outside of MS Azure. This API allows developers and the support team to trigger retries for failed internal system messages that Azure has moved to a poison queue.
- Monthly Bulk Match (MBM) module: This is an internal FNS NAC process; it is not exposed outside of Azure. This module operates on a timer and identifies all instances of duplicate participation in the FNS NAC and generates corresponding match records for each instance. At the end of processing, States are provided with an email, via the Notification App, containing a link to their report of the month's identified matches in the Query Tool MBM App.
- Query Tool MBM App: Provides a way for authorized members of state agencies to review, filter, & sort MBM information via a web interface. Also allows members to resolve MBM matches.
- USDA eAuth: Authenticates users who interact with the FNS NAC directly, through the FNS NAC Query App and FNCS Dashboard. Ensures that only authorized users have access to each application.

Section 11(x) of the Food and Nutrition Act (7 U.S.C. 2020(x)) requires FNCS to establish the FNS NAC.

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?

Section 11(x) of the Food and Nutrition Act (7 U.S.C. 2020(x)) requires FNCS to build and maintain the FNS NAC to prevent individuals from receiving Supplemental Nutrition Assistance Program (SNAP) benefits in more than one State simultaneously, also known as duplicate participation. As a federal matching program, FNCS and State agencies are subject to the further provisions provided in the Computer Matching Agreement (CMA) as required and defined by the Privacy Act.

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

Yes, with an initial ATO issued on 12/02/2021 and an ATO update due to a significant change issued on 1/18/2023. The ATO is currently valid through 11/30/2026.

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

USDA/FNS-14, National Accuracy Clearinghouse (FNS NAC)

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

N/A

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
□	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 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

Identifying Numbers					
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

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

The data about is collected by the State agencies, directly from participants and applicants.

2.2.1. How is the information collected?

The data about SNAP participants is collected by the State agencies, directly from participants and applicants. The case information is generated by State agencies as they administer the program. The State agency business email and business telephone data is collected by the State Agencies. The information is shared to the FNS NAC by State agencies.

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

N/A

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

State agencies supply and verify for accuracy, relevance, timeliness and completeness of the data collected and shared based on strict specifications provided by FNCS. This is particularly important for the PII fields that are de-identified as FNCS only receives their secure hash. FNCS does verify the completeness and basic checks on the data types to ensure they are correct.

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?

The FNS NAC does not include any 3rd party websites or applications for the public to use.

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

N/A

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

Privacy Risk: The following privacy risks to individuals have been identified:

- Disclosure of personal information of SNAP participants that could be used for identity theft (name, date of birth, social security number).
- Disclosure of limited SNAP case information, including household composition and the state in which a participant resides.
- Revealing that an individual is a SNAP participant.
- Disclosure of limited State Agency information, business email and business phone.

Mitigation: To mitigate these risks, FNCS has taken the following key actions:

- **Limiting the sensitive data that is collected and stored**. FNCS obtains from State Agencies only the minimum amount of sensitive data needed to meet statutory requirements.
- **Maintaining participant data only as long as it is needed**. State agencies provides information on active SNAP participants daily. New information provided by State agencies supplants the prior information, in effect purging information on individuals who cease to be SNAP participants because their information is not needed to meet the system purpose of preventing duplicate participation. Participants who were involved in a match will have their information removed after a satisfactory retention period to monitor ongoing program integrity.
- **Limiting access to the system and data**. Users are only provided with access to the features and data needed within their assigned role. State agency workers have access to perform queries and see matches in their state, but do not have access to system performance metrics. Similarly, FNCS staff members have access to monitor system metrics but do not have the ability to look up the de-identified PII for individuals involved in a match. The FNS NAC does not provide a method for users to see the list of SNAP participants, browse them, or export them. Access to PII is only provided for participants who have been identified in a multi-state match.
- **Encrypting sensitive data**. Data is encrypted while being transmitted between the State agencies and FNCS, and while being stored by FNCS.
- **Monitoring the security of the data and supporting systems on a continuous basis**. FNCS has established a robust information security continuous monitoring program that includes the design, implementation, monitoring, and independent assessment of the security

and privacy controls protecting the FNS NAC system and data. This includes ensuring that clear roles and responsibilities for data protection are established between FNCS and each participating State Agency.

- **De-identified PII.** This de-identification technique is part of an approach called Privacy-Preserving Record Linkage (PPRL). PPRL is a process that identifies and links records that correspond to the same individual across different databases, without revealing private information to the linking organization. As a result, the FNS NAC does not directly store sensitive PII. The de-identification process protects against SNAP participant PII (specifically name, DOB, and SSN) being exposed or used for purposes other than those specified by the 2018 Farm Bill. It is theoretically possible that a sophisticated attacker with nation-state resources could exfiltrate the de-identified information stored in the FNS NAC to re-identify PII of SNAP participants, but this risk is greatly reduced through access controls and encryption.

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 FNS NAC is a tool to help State agencies prevent duplicate participation in SNAP. State agencies conduct matches against the FNS NAC of individuals who have applied or are being recertified for SNAP benefits. This information is compared to information provided by other State agencies about SNAP participants to determine if the individual is receiving SNAP benefits in another State. When a match is found, State agencies are provided with notification that includes a unique Match ID, State case ID, State participant ID, and other non-PII case meta data (vulnerable individual flag, recent benefit dates, case closure date, if applicable) in order for the other State to assist with verification of the match. It does not include the PII fields of name, DOB, and SSN, as the FNS NAC does not collect this information. State agencies use this information to take action to prevent or end duplicate participation.

FNCS uses information generated by the FNS NAC for the sole purpose of monitoring program integrity and the integrity of the system.

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.

This system uses custom built tools to evaluate metrics of system performance. These metrics are aggregated and do not contain PII. Examples include the last time when a state updated its enrollment data and the percentage of matches that are found to be false positives.

The system integrates with centralized logging tools for auditing system access and detection of faults. This may include detailed error messages for any system operation, but care is taken to avoid inclusion of PII in those log files.

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

Privacy Risk: The following privacy risks to individuals have been identified:

- Disclosure of personal information of SNAP participants that could be used for identity theft (name, date of birth, social security number).
- Disclosure of limited SNAP case information, including household composition and the state in which a participant resides.
- Revealing that an individual is a SNAP participant.
- Disclosure of limited State Agency information, business email and business phone.

Mitigation: To mitigate these risks, FNCS has taken the following key actions:

- **Limiting the sensitive data that is collected and stored**. FNCS obtains from State Agencies only the minimum amount of sensitive data needed to meet statutory requirements.
- **Maintaining participant data only as long as it is needed**. State agencies provide information on active SNAP participants daily. New information provided by State agencies supplants the prior information, in effect purging information on individuals who cease to be SNAP participants because their information is not needed to meet the system purpose of preventing duplicate participation. Participants who were involved in a match will have their information removed after a satisfactory retention period to monitor ongoing program integrity.
- **Limiting access to the system and data**. Users are only provided with access to the features and data needed within their assigned role. State agency workers have access to perform queries and see matches in their state, but do not have access to system performance metrics. Similarly, FNCS staff members have access to monitor system metrics but do not have the ability to look up de-identified PII for individuals involved in a match. The FNS NAC does not provide a method for users to see the list of SNAP participants, browse them, or export them. Access to PII is only provided for participants who have been identified in a multi-state match.
- **Encrypting sensitive data**. Data is encrypted while being transmitted between the State agencies and FNCS, and while being stored by FNCS.
- **Monitoring the security of the data and supporting systems on a continuous basis**. FNCS has established a robust information security continuous monitoring program that includes the design, implementation, monitoring, and independent assessment of the security and privacy controls protecting the FNS NAC system and data. This includes ensuring that clear roles and responsibilities for data protection are established between FNCS and each participating State Agency.

- **De-identified PII.** This de-identification technique is part of an approach called Privacy-Preserving Record Linkage (PPRL). PPRL is a process that identifies and links records that correspond to the same individual across different databases, without revealing private information to the linking organization. As a result, the FNS NAC does not directly store sensitive PII. The de-identification process protects against SNAP participant PII (specifically name, DOB, and SSN) being exposed or used for purposes other than those specified by the 2018 Farm Bill. It is theoretically possible that a sophisticated attacker with nation-state resources could exfiltrate the de-identified information stored in the FNS NAC to re-identify PII of SNAP participants, but this risk is greatly reduced through access controls and encryption.
- **Additional mitigations.** Access to the FNS NAC system and data obtained is tightly controlled through the use of eAuthentication. Users are assigned roles within the system to limit their access to data. All data is encrypted at rest and in transit. The FNS NAC adheres to all applicable privacy controls from NIST SP 800-53 (Rev. 5) to ensure that PII is handled properly. Control AT-03(05), from NIST Special Publication 800-53 (Rev. 5), requires all users to be trained in the proper use and handling of PII. Security awareness training is required for FNCS new users, and on an annual basis, and is provided by FNCS. Additionally, FNCS adheres to control PM-25 from NIST Special Publication 800-53 (Rev. 5) which requires the minimization of PII used in testing, training, and research and is documented in the associated System Security Plan. Moreover, FNCS has implemented a periodic review of publicly accessible sites to ensure that no sensitive data is accessible. Furthermore, the PII entered into the FNS NAC is de-identified. Therefore, the FNS NAC does not directly store sensitive PII. This de-identification process further protects SNAP participant. Additional controls are specified in section 2.6 above.

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 must provide information about the required data collection on the SNAP application at the time of application and recertification.

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

Applicants are notified of the uses of the information at application and recertification; however, refusal to provide required information to the State agency will result in the denial of SNAP benefits.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Privacy Risk: The risk of individuals being unaware of the collection.

Mitigation: State agencies must notify all households applying and being recertified for SNAP benefits of the following information per 7 CFR 273.2(b)(4). The collection of this information, including the social security number (SSN) of each household member, is authorized under the Food and Nutrition Act of 2008, as amended, 7 U.S.C. 2011-2036. The information is used to determine whether the household is eligible or continues to be eligible to participate in SNAP. This information is verified through computer matching programs. This information is also used to monitor compliance with program regulations and for program management.

The risk of individuals being unaware of the collection are mitigated by providing the information at application and each time their case comes up for recertification.

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?

Section 11(x)(C) of the Food and Nutrition Act establishes data protection that includes maintaining information only as long as is necessary to accomplish the system purpose of preventing duplicate participation. As such, PII and case information records provided by State agencies to populate the FNS NAC database/master file (retention requirements being proposed to NARA for approval) will be retained until they are superseded by a new upload from the State agency, usually daily, to ensure matches are conducted against information related to current participants.

When positive matches are found, the related records will be retained in the FNS NAC for up to three (3) years from the match date to monitor program integrity efforts related to duplicate participation.

Other non-PII records maintained for audit or oversight purposes will be retained for three (3) years from the date provided to or generated by the system.

Summary or aggregate data maintained for reporting and oversight purposes will be retained in the system indefinitely.

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.

The FNS NAC does not have a NARA-approved records schedule at this time.

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

Privacy Risk: FNS does not have an established length of time to retain PII due to the federal statue allowing records to be kept "as long as is necessary to accomplish the system purpose of preventing duplicate participation". The length of time FNS is allowed to keep the information per federal statue establishes the following privacy risks in regard to the retention of sensitive data:

- Disclosure of personal information of SNAP participants that could be used for identity theft (name, date of birth, social security number).
- Disclosure of limited SNAP case information, including household composition and the state in which a participant resides.
- Revealing that an individual is a SNAP participant.
- Disclosure of limited State Agency information, business email and business phone.

Mitigation: To mitigate these risks, FNCS has taken the following key actions:

- **Limiting the sensitive data that is collected and stored**. FNCS obtains from State Agencies only the minimum amount of sensitive data needed to meet statutory requirements.
- **Maintaining participant data only as long as it is needed**. State agencies provide information on active SNAP participants daily. New information provided by State agencies supplants the prior information, in effect purging information on individuals who cease to be SNAP participants because their information is not needed to meet the system purpose of preventing duplicate participation. Participants who were involved in a match will have their information removed after a satisfactory retention period to monitor ongoing program integrity.
- **Limiting access to the system and data**. Users are only provided with access to the features and data needed within their assigned role. State agency workers have access to perform queries and see matches in their state, but do not have access to system performance metrics. Similarly, FNCS staff members have access to monitor system metrics but do not have the ability to look up de-identified PII for individuals involved in a match. The FNS NAC does not provide a method for users to see the list of SNAP participants, browse them, or export them. Access to PII is only provided for participants who have been identified in a multi-state match.
- **Encrypting sensitive data**. Data is encrypted while being transmitted between the State Agencies and FNCS, and while being stored by FNCS.
- **Monitoring the security of the data and supporting systems on a continuous basis**. FNCS has established a robust information security continuous monitoring program that includes the design, implementation, monitoring, and independent assessment of the security and privacy controls protecting the FNS NAC system and data. This includes ensuring that clear roles and responsibilities for data protection are established between FNCS and each participating State Agency.

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?

Information in the FNS NAC is shared within USDA only with those staff members and contractors, or others with whom FNCS has established a legal relationship, who require access as part of the system development and maintenance team or to perform their duties in the administration of SNAP.

Information is not transmitted internally. Access to the system information is provided to individuals based on their permission level as indicated on their FNS-674. These permission levels are determined based on the level of access needed to perform their job duties.

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

Privacy Risk: The following privacy risks have been identified regarding the retention of sensitive data:

- Disclosure of personal information of SNAP participants to individuals without a requirement for access.
- Disclosure of limited SNAP case information, including household composition and the state in which a participant resides, to individuals without a requirement for access.

Mitigation: To mitigate these risks, FNCS has taken the following key actions:

- **Limiting access to the system and data**. Users are only provided with access to the features and data needed within their assigned role. State agency workers have access to perform queries and see matches in their state, but do not have access to system performance metrics. Similarly, FNCS staff members have access to monitor system metrics but do not have the ability to look up de-identified PII for individuals involved in a match. The FNS NAC does not provide a method for users to see the list of SNAP participants, browse them, or export them. Access to PII is only provided for participants who have been identified in a multi-state match.
- **Encrypting sensitive data**. Data is encrypted while being transmitted between the State Agencies and FNCS, and while being stored by FNCS.
- **Monitoring the security of the data and supporting systems on a continuous basis**. FNCS has established a robust information security continuous monitoring program that includes the design, implementation, monitoring, and independent assessment of the security and privacy controls protecting the FNS NAC system and data. This includes ensuring that clear roles and responsibilities for data protection are established between FNCS and each participating State Agency.

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?

State agencies that are responsible for administering SNAP are the primary users of the FNS NAC. Its purpose is to provide them with a method to access information about SNAP participation in other States to prevent duplicate participation. State agencies conduct matches against the FNS NAC by providing information about individuals who have applied or are being recertified for SNAP. This information is compared to information provided by other State agencies about SNAP participants. When a match is found, State agencies are provided with notification that includes a unique match ID, generated by the FNS NAC, which does not include PII.

State agencies are then able to use this match ID to retrieve the match record within the FNS NAC, which contains information to help them resolve the match. This information includes participant ID and may include case ID, vulnerable individual flag, case closure date, and recent benefit months. State agencies use the participant ID and the case ID to find the matched individual within their own state benefits system.

Access to the FNS NAC APIs that permit information sharing is limited to systems that possess access credentials that are only made available to State agencies for the purpose of integrating the FNS NAC into their benefits administration systems.

Access to the FNS NAC search website for users outside the Department is limited to users at state agencies who have an approved FNS-674. These users must verify their identity by logging in through eAuth.

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

Privacy Risk: The following privacy risks to individuals have been identified:

- Disclosure of personal information of SNAP participants that could be used for identity theft (name, date of birth, social security number)
- Disclosure of limited SNAP case information, including household composition and the state in which a participant resides.
- Revealing that an individual is a SNAP participant.

Mitigation: To mitigate these risks, FNCS has taken the following key actions:

- **Limiting the sensitive data that is collected and stored**. FNCS obtains from State Agencies only the minimum amount of sensitive data needed to meet statutory requirements.
- **Maintaining participant data only as long as it is needed**. State agencies provide information on active SNAP participants daily. New information provided by State agencies supplants the prior information, in effect purging information on individuals who cease to be SNAP participants because their information is not needed to meet the system purpose of

preventing duplicate participation. Participants who were involved in a match will have their information removed after a satisfactory retention period to monitor ongoing program integrity.

- **Limiting access to the system and data**. Users are only provided with access to the features and data needed within their assigned role. State agency workers have access to perform queries and see matches in their state, but do not have access to system performance metrics. Similarly, FNCS staff members have access to monitor system metrics but do not have the ability to look up de-identified PII for individuals involved in a match. The FNS NAC does not provide a method for users to see the list of SNAP participants, browse them, or export them. Access to PII is only provided for participants who have been identified in a multi-state match.
- **Encrypting sensitive data**. Data is encrypted while being transmitted between the State Agencies and FNCS, and while being stored by FNCS.
- **Monitoring the security of the data and supporting systems on a continuous basis**. FNCS has established a robust information security continuous monitoring program that includes the design, implementation, monitoring, and independent assessment of the security and privacy controls protecting the FNS NAC system and data. This includes ensuring that clear roles and responsibilities for data protection are established between FNCS and each participating State Agency.

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?

Personal information contained in this system is provided by the State agency where the individual is a SNAP participant or applicant. Individuals may obtain information about records in the system pertaining to them by submitting a written request to the System Owner listed below. The envelope and the letter should be marked "Privacy Act Request," and should include the name, date of birth, State where the individual received benefits, and social security number of the individual for which the request is made.

Requests to the System Owner must also include sufficient data for FNCS to verify your identity. If the sensitivity of the records warrants it, FNCS may require that you submit a signed, notarized statement indicating that you are the individual to whom the records pertain and stipulating that you understand that knowingly or willfully seeking or obtaining access to records about another individual under false pretenses is a misdemeanor punishable by fine up to $5,000. No identification shall be required, unless the records are required by 5 U.S.C. 552 to be released. If FNCS determines to grant the requested access, fees may be charged in accordance with § 1.120 before making the necessary copies. In place of a notarization, your signature may be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization.

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

Individuals desiring to contest or amend information maintained in the system may direct their requests to the System Owner listed below or to the State agency that provided the data to the FNS NAC. Requests sent to the System Owner should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. Requests sent to the System Owner will be shared to the State agency that provided the data for resolution.

FNCS is not able to change information about individuals within the FNS NAC. State agencies serve as the authoritative source for the information they provide and are accountable for providing accurate information from their system to the FNS NAC.

In addition, if an applicant or participant disagrees with any action taken on a SNAP case in response to information received from a FNS NAC match, the individual may request a fair hearing with the State agency to dispute the decision.

System Owner Contact Information:

Director, Portfolio Management Division,
Office of Information Technology, Food and Nutrition Service,
Privacy Act Request
1320 Braddock Road, Alexandria, Virginia 22314.
Telephone: (703) 305–2504.

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

Individuals are notified via the USDA/FNS–14, Supplemental Nutrition Assistance Program (SNAP), National Accuracy Clearinghouse (NAC) System to Detect Duplicate Participation System of Records Notice published to the federal register. The notice informs household of their right to a hearing, of the method by which a hearing may be requested, and that its case may be presented by a household member or a representative, such as a legal counsel, a relative, a friend or other spokesperson. In addition, at any time the household expresses to the State agency that it disagrees with a State agency action, it shall be reminded of the right to request a fair hearing.

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

None.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Privacy Risk: Households may not understand they must submit their request to correct inaccurate or erroneous in writing.

Mitigation: This PIA along with the USDA/FNS–14, Supplemental Nutrition Assistance Program (SNAP), National Accuracy Clearinghouse (NAC) System to Detect Duplicate Participation System of Records Notice provides individuals with clear instructions that all request to correct inaccurate or erroneous in writing must be submitted in writing to the System Owner via mail to:

Director, Portfolio Management Division,

Office of Information Technology, Food and Nutrition Service,
Privacy Act Request
1320 Braddock Road, Alexandria, Virginia 22314.

The request must include the name, date of birth, and state where the individual received benefits, and social security number of the individual for which the request is made.

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?

Data is encrypted while being transmitted between the State Agencies and FNCS, and while being stored by FNCS.

FNCS has established a robust information security continuous monitoring program that includes the design, implementation, monitoring, and independent assessment of the security and privacy controls protecting the FNS NAC system and data. This includes ensuring that clear roles and responsibilities for data protection are established between FNCS and each participating State Agency. The system is designed for defense-in-depth and a Zero Trust model, on top of a privacy-preserving record linkage (PPRL) approach that limits plain text PII to the per-state participant ID. Components/services within the system are granted only the access rights required. There are cloud platform mechanisms to help prevent data exfiltration, including limits to the amount of data that can be retrieved in a single query, per-state, isolated datastores, network segregation, and intrinsic technical limits on backups / restores. All communications are over encrypted channels. PII and de-identified PII are encrypted at the application level (e.g., database column) as well as at rest.

Access to the FNS NAC system and data obtained is tightly controlled through the use of eAuthentication. Users are assigned roles within the system to limit their access to data. All data is encrypted at rest and in transit.

Each request to retrieve data containing PII is logged and includes the identity of requesting system/system user, time of event, and other event data. This event logging occurs when a state system accesses the APIs, when a query is made through the FNS NAC query tool, or in the rare event an internal super user directly accesses internal system resources and is designed to support coordinated investigations with the State agencies. All events are sent to a Security Information and Event Management (SIEM) for aggregate analysis for indicators of compromise.