USDA Privacy Impact Assessment

Fiscal Year 2025

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Template Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed "Gender" and "Sexual Orientation" from Biographical Information in accordance with Executive Order 14168, "Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government."

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	SNAP Information Database
Program Office	Office of Information Technology
Mission Area	Food, Nutrition, and Consumer Services
CSAM Number	1176 - FNCS Infrastructure Services General Support System (FNCS I-GSS)
Date Submitted for Review	06/01/2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Deea Coleman	Deea.Coleman@usda.gov	None
Information System Security Manager	John Rosselot, Jr.	John.Rosselotjr@usda.gov	None
System/Program Managers	Gina Brand	Gina.Brand@usda.gov	None

Abstract

The abstract provides the simplest explanation to the question “what does the project, application, or system do?” and will be published online to accompany the PIA link.

The SNAP Information Database is an initiative of USDA’s Office of the Secretary that will leverage data-sharing across federal and state systems to identify and rectify any ineligible, duplicate, or fraudulent Supplemental Nutrition Assistance Program (SNAP) enrollments. In addition, this initiative will focus on detecting duplicate enrollments across states, verifying immigration status eligibility, and performing other fraud prevention checks using lawfully shared internal and interagency data across a number of Federal agencies. The SNAP Information Database will collect SNAP participant data (including personal information and transactional data) from all 53 SNAP state agencies via their Electronic Benefit Transfer (EBT) payment processors, through secure channels, to be stored in a database that is then used to perform integrity checks that include, but may not be limited to:

- Duplicate enrollment (multi-state);
- Identity and social security number (SSN) validation;
- Immigration status check;
- Age and household composition validation; and
- Inter-Agency data matches

Integrity checks will be executed using automated scripts and queries on the compiled database, using matching algorithms to minimize false positives. States will transmit data from 2020 to present, with quarterly updates thereafter.

A Privacy Impact Assessment (PIA) is required due to the storage and use of personally identifiable information by the SNAP Information Database.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

The USDA Office of the Secretary will establish the SNAP Information Database in the Food and Nutrition Service (FNS) Amazon Web Services (AWS) environment. FNS’ Office of Information Technology (OIT) maintains a secure AWS environment that is authorized under the FNS Infrastructure General Support System (FNS I-GSS) Authority to Operate (ATO).

Data will be sent via the secure MoveIt or Box managed file transfer application. SNAP participant data to be contained in the SNAP Information Database will include detailed and sensitive personally identifiable information (PII) which is required to perform the integrity checks as designed, as well as financial data (e.g., amount of benefit received). Data from all participants since 2000 to present will be collected, with quarterly updates submitted by states or their EBT processors thereafter.

As part of the integrity initiative, USDA will leverage data-sharing across federal and state systems to identify and rectify any ineligible, duplicate, or fraudulent SNAP enrollments or transactions. This also includes sharing, where permitted by law and consistent with this notice, information with State agencies when necessary to investigate and rectify fraudulent or otherwise improper or illegal SNAP enrollments or transactions.

The collection of PII is authorized in 7 U.S.C. § 2204: USDA/FNS possesses the legal authority to collect and utilize SNAP beneficiary data for program administration and enforcement as provided, for example, in the Food and Nutrition Act of 2008 (7 U.S.C. 2011 et seq.) at 7 U.S.C. 2020(a)(3)(B), e(8)(A); 7 C.F.R. 272.1(c)(1), (e).

Section 1: Authorities and Other Requirements

These questions identify all statutory and regulatory authorities for operating the project, application, or system, including the authority for collection, which 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, application, or system?

7 U.S.C. § 2204. USDA/FNS possesses the legal authority to collect and utilize SNAP beneficiary data for program administration and enforcement as provided, for example, in the Food and Nutrition Act of 2008 (7 U.S.C. 2011 et seq.) at 7 U.S.C. 2020(a)(3)(B), e(8)(A); 7 C.F.R. 272.1(c)(1), (e)

1.2. Has Authorization and Accreditation (A&A) been completed for the project, application, or system?

The SNAP Information Database does not have a complete A&A, however the AWS environment that will house the database has an ATO that expires 09/30/2025 and the annual A&A is ongoing.

1.3. Which System of Records Notices (SORNs) apply to the information?

USDA/FNS-15, "National Supplemental Nutrition Assistance Program (SNAP) Information Database. https://www.federalregister.gov/documents/2025/06/23/2025-11463/privacy-act-of-1974-system-of-records

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

The Paperwork Reduction Act applies to this collection of information. Collection and recordkeeping of these elements was previously approved under OMB Control #0584-0064; a change request is in process to reflect the marginal increase in reporting burden necessary to populate the database.

Section 2: Information Characterization

These questions define the scope of the information requested and collected, as well as the reasons for its collection as part of the project, application, or system being developed:

2.1. What information is collected, used, disseminated, or maintained in the project, application, or system? Select all applicable Personally Identifiable Information (PII) and data elements that your project, application, or system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, list it in the text box at the end of this section.

Note: 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.

Identifying Numbers

☒ Social Security Number	☐ Truncated or Partial Social Security Number	☐ Driver's License Number
☐ Passport Number	☐ License Plate Number	☐ Registration Number
☒ File or Case ID Number	☐ Student ID Number	☐ Federal Student Aid Number
☒ Employee Identification Number	☒ Alien Registration Number	☐ Department of Defense Identification Number
☐ Professional License Number	☐ Taxpayer Identification Number	☐ Business Taxpayer Identification Number (Sole Proprietor)
☒ EBT 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 Phone Number
☐ Health Plan Beneficiary Number	☐ Business Mobile Phone Number (Sole Proprietor)	☐ Department of Defense Benefits Number

Biographical Information

☒ Name (Including Nicknames)
☐ Business Mailing Address (Sole Proprietor)
☒ Date of Birth
☐ Ethnicity
☐ Business Phone or Fax Number (Sole Proprietor)
☐ Country of Birth
☐ City or County of Birth
☐ Group or Organization Membership
☐ Religion or Religious Preference
☒ Citizenship
☒ Immigration Status
☐ Home Phone or Fax Number
☒ Home Address
☒ ZIP Code
☒ Marital Status
☒ Spouse Information
☐ Child Information
☐ Military Service Information
☐ Race
☐ Nationality
☐ Mother's Maiden Name
☐ Personal Email Address
☐ Business Email Address
☐ Global Positioning System (GPS) or Location Data
☒ Employment Information
☐ Alias (Username or Screenname)
☐ Personal Financial Information (Including Loan Information)
☒ Education Information
☐ Resume or Curriculum Vitae
☐ Business Financial Information (Including Loan Information)
☐ Professional or Personal References

Biometrics

☐ Fingerprints
☐ Hair Color
☐ DNA Sample or Profile
☐ Retina or Iris Scans
☐ Video Recording

Distinguishing Features

☐ Palm Prints
☐ Eye Color
☐ Signatures
☐ Dental Profile
☐ Photos

Characteristics

☐ Vascular Scans
☐ Height
☐ Weight
☐ Scars, Marks, or Tattoos
☐ Voice or Audio Recording

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, or Ringtones)
☐ Cell Tower Records (e.g., Logs, User Location, or Time)
☐ Network Communication Data

Medical and Emergency Information

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

Specific Information and File Types

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

[List additional information collected but not listed above here (for example, a personal phone number that is used as a business number).]

2.2. What are the sources of the information in the project, application, or system?

This data is collected and maintained by 53 SNAP State agencies and EBT processors, under contract with the State. States and EBT processors will transmit this information to FNS for the SNAP Information Database.

2.2.1. How is the information collected?

PII is collected by the States per the Food and Nutrition Act of 2008.

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

No

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

USDA will cross check data against other Federal databases using matching algorithms to determine accuracy.

2.5. Does the project, application, or system use third-party websites?

No

2.5.1. What is the purpose of the use of third-party websites?

Not applicable.

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

None.

Privacy Impact Analysis

2.6. List the privacy risks and mitigations related to the characterization of the information.

Privacy Risk: Privacy Act risks associated with the characterization of SNAP Information Database information may include:

- **Over-collection of Data:** Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.
- **Non-compliance with Regulations:** Failing to accurately characterize information can lead to non-compliance with privacy laws and regulations, resulting in legal penalties and reputational damage.
- **Lack of Individual Awareness:** If individuals are not informed about how their PII is characterized and used, it can lead to a lack of trust and potential backlash against the organization.
- **Failure to Honor Individual Rights:** Mischaracterization may lead to difficulties in fulfilling individual rights requests, such as access or deletion, if the organization does not accurately track how data is categorized and used.

Mitigation: Addressing risks through proper data characterization practices is essential for maintaining compliance with the Privacy Act and protecting individuals' personal information. By implementing the following mitigation actions, the SNAP Information Database can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the Privacy Act requirements.

- **Regular Data Inventory:** Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.
- **Individual Consent for Sensitive Data:** Obtain explicit consent for the collection and processing of sensitive personal information, such as health or financial data, and ensure that individuals are aware of its characterization.
- **Regular Data Inventory:** Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Section 3: Information Uses

These questions 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 project, application, or system's business purpose.

The PII collected from the states and used by the SNAP Information Database is required to detect duplicate enrollments across states, verify immigration status eligibility, and perform other fraud prevention checks against other Federal agencies' datasets, thereby ensuring program integrity, including by verifying the eligibility of benefit recipients.

3.2. Does the project, application, or system 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..

USDA will use the SNAP data to ensure the integrity of Government programs, including by verifying SNAP recipient eligibility against federally maintained databases. This is consistent with USDA's statutory authority and will ensure Americans in need receive assistance, while at the same time safeguarding taxpayer dollars from abuse. USDA will leverage data-sharing across Federal and State systems to identify and rectify any ineligible, duplicate, or fraudulent SNAP enrollments or transactions. This includes verifying eligibility based on immigration status, identifying and eliminating duplicate enrollments, assisting States in mitigating identity theft, and performing other eligibility and program integrity checks using lawfully shared internal and interagency data. This also includes sharing, where permitted by law and consistent with this notice, information with State agencies when necessary to investigate and rectify fraudulent or otherwise improper or illegal SNAP enrollments or transactions.

Privacy Impact Analysis

3.3. List the privacy risks and mitigations related to uses of the information.

Privacy Risk: Privacy act risks associated with the uses of information by the SNAP Information Database include:

- **Purpose Limitation:** Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.
- **Unauthorized Use of Data:** PII may be used for purposes other than those for which it was collected, violating privacy principles and individual expectations.
- **Data Misuse:** Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

- **Inadequate Consent:** If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.
- **Overuse of Information:** Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.
- **Loss of Data Control:** When PII is shared with third parties, there is a risk of losing control over how that data is used, potentially leading to unauthorized access or exploitation.
- **Increased Risk of Data Breaches:** The more PII is used and shared, the higher the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.
- **Negative Impact on Reputation:** Misusing PII can harm the agency's reputation, leading to loss of customer trust and potential business losses.
- **Failure to Honor Individual Rights:** Inadequate processes for managing the use of PII may result in the inability to fulfill individual rights requests, such as access, correction, or deletion.
- **Compliance Violations:** Using information in ways that are not compliant with privacy acts can lead to legal penalties, audits, and increased scrutiny from regulators.

Mitigation: By implementing some or all the following mitigation actions, the SNAP Information Database may better safeguard PII and ensure responsible use in compliance with Privacy Act requirements:

- **Monitoring and Auditing:** Regularly monitor and audit the use of personal information to ensure compliance with privacy policies and identify any unauthorized or inappropriate uses.
- **Data Minimization:** Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.
- **Regular Training:** Provide regular training for employees on privacy laws and the importance of adhering to the defined uses of personal information to ensure compliance.
- **Individual Consent:** Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

- **Transparency:** Inform individuals about how their personal information will be used, including any potential secondary uses, through clear and accessible privacy notices.
- **Access Controls:** Implement access controls to restrict who can use personal information and for what purposes, ensuring that only authorized personnel have access to sensitive data.
- **Incident Response Plan:** Follow department incident response plan to address any misuse of PII, outlining procedures for reporting and mitigating such incidents.
- **Privacy Impact Assessments (PIAs):** Conduct PIAs for new projects or uses of PII to assess potential risks to privacy and implement measures to mitigate them.
- **Individual Rights Awareness:** Make individuals aware of their rights regarding their personal information, including the right to access, correct, or request deletion of their data.

Section 4: Notice

These questions are intended to provide 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, application, or system provide notice to individuals prior to collection?

States provide notice at the point the individual applies for SNAP enrollment.

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

Notice for an individual's consent, decline, or opt out of the data collection is the responsibility of the State administering the SNAP enrollment.

Privacy Impact Analysis

4.3. List the privacy risks and mitigations related to notice. Follow this format:

Privacy Risk: States will transmit their respective collected data, inclusive of PII, to the SNAP Information Database. As such, notice for the collection of PII falls within the state's responsibility. Privacy Act risks associated with notices include:

- **Inadequate Disclosure:** Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.
- **Ambiguity:** If notices are unclear or overly complex, individuals may not fully understand their rights or the SNAP Information Database's data practices, leading to a lack of informed consent.
- **Non-Compliance with Regulations:** Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.
- **Insufficient Updates:** Notices that are not regularly updated to reflect changes in data practices or legal requirements can mislead individuals and result in privacy violations.
- **Lack of Accessibility:** Notices that are not easily accessible or understandable to all individuals, including those with disabilities or language barriers, can lead to exclusion and non-compliance.
- **Failure to Communicate Changes:** Not adequately informing individuals about changes to privacy practices or policies can lead to confusion and mistrust, especially if data practices evolve.

- **Over-collection of Data:** If notices do not clearly explain the purpose of data collection, individuals may be more likely to provide information that is not necessary, leading to potential data minimization violations.
- **Inconsistent Messaging:** Different notices provided by various states may contain conflicting information, causing confusion and undermining trust.
- **Underestimating Individual Rights:** Notices that do not clearly outline individuals' rights regarding their personal information can prevent them from exercising those rights effectively.

Mitigation: Implementing some or all the following mitigation actions, the SNAP Information Database, and by extension states, can better protect individual privacy rights and comply with privacy act requirements:

- **Clear Communication:** Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all individuals.
- **Regular Updates:** Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.
- **Feedback Mechanism:** Establish a process for individuals to ask questions or express concerns about privacy notices and practices, allowing for continuous improvement.
- **Individual Consent:** Implement mechanisms for obtaining explicit individual consent for data collection and processing and provide options for individuals to withdraw consent easily.
- **Transparency:** Clearly outline what personal data is being collected, the purpose of data collection, how it will be used, and who it will be shared with.
- **Data Minimization:** Limit data collection to only what is necessary for the stated purpose. Avoid collecting excessive or irrelevant data.
- **Individual Rights:** Inform individuals about their rights regarding their personal data, including access, correction, deletion, and the ability to object to processing.
- **Accessibility:** Make privacy notices easily accessible on websites and apps, ensuring they can be found without difficulty.
- **Third-Party Compliance:** Ensure that any third parties handling personal data adhere to the same privacy standards and practices as outlined in their privacy notices.

Section 5: Data Retention

These questions outline how long information will be retained after the initial collection.

5.1. What information is retained and for how long?

Records are retained and disposed of in accordance with Section 11(a)(3)(B) of the FNA. Records may be retained for a period of not less than 3 years as specified in the FNA or applicable regulation, or for a longer period as required by litigation, investigation, and/or audit. Electronic records are retained by FNS employees and contractors at FNS offices.

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

This system does not yet have a NARA-approved records schedule. All records in this system will be kept indefinitely unless otherwise required by law until NARA has approved a records schedule for this system.

Privacy Impact Analysis

5.3. List the privacy risks and mitigations related to data retention. Follow this format:

Privacy Risk: Privacy act risks associated with the retention of information within the SNAP Information Database include:

- **Excessive Data Retention:** Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.
- **Data Breaches:** The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.
- **Non-compliance with Regulations:** Failing to adhere to legal requirements regarding data retention periods can lead to regulatory penalties and legal liabilities.
- **Obsolescence of Data:** Retained data may become outdated or irrelevant, leading to inaccuracies in decision-making or service delivery, which can affect individuals negatively.
- **Inadequate Disposal Procedures:** If the SNAP Information Database does not have secure methods for disposing PII that is no longer needed, it can lead to unintended exposure of sensitive data.

- **Inconsistent Retention Practices:** Different states or external federal agencies with which SNAP Information Database data is shared may follow varying retention practices, resulting in confusion and potential violations of privacy policies.
- **Failure to Honor Individual Requests:** Retaining information longer than necessary may hinder the SNAP Information Database's ability to fulfill individual requests for data deletion or access, leading to dissatisfaction and potential legal issues.
- **Increased Legal Risks:** Long retention periods can increase the risk of being involved in litigation, as older data may be subjected to subpoenas or discovery requests.
- **Reputation Damage:** Inadequate retention practices can lead to public relations issues and damage a department's reputation if PII is mishandled or exposed.
- **Lack of Accountability:** Without proper oversight of retention practices, there may be a lack of accountability for data management, increasing the risk of errors and privacy violations.

Mitigation: Implementing the following mitigation actions, the SNAP Information Database can ensure responsible retention of PII while complying with the Privacy Act.

- **Data Retention Policy:** Use NARA data retention policies that outlines how long different types of PII will be retained and the rationale for those timeframes.
- **Data Minimization:** Collect and retain only the PII that is necessary for the intended purpose, minimizing the risk associated with holding excessive data.
- **Regular Reviews:** Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.
- **Access Controls: I**mplement strict access controls to limit who can view and manage retained personal information, reducing the risk of unauthorized access.
- **Audit Trail:** Maintain an audit trail to document when data is collected, accessed, and disposed of, which can help demonstrate compliance with retention policies.
- **Compliance Checks:** Regularly conduct compliance checks to ensure that retention practices align with legal requirements and organizational policies.

- **Retention Schedule:** Follow a retention schedule that specifies the duration for retaining different types of records and when they should be reviewed or disposed of.
- **Secure Disposal Procedures:** Establish secure methods for the disposal of personal information that is no longer needed, such as shredding paper documents or using data-wiping software for electronic files.
- **Documentation and Training:** Ensure that employees are aware of and trained on the data retention policy, including the importance of compliance and the procedures for handling personal information.
- **Individual Rights Notification:** Inform individuals about their rights regarding data retention, including the right to request deletion of their personal information when it is no longer necessary for the purposes for which it was collected.

Section 6: Information Sharing

These questions define the content, scope, and authority for information sharing.

Internal Information Sharing

6.1. With which internal organizations and/or systems is information shared, received, and/or transmitted? What information is shared, received, and/or transmitted, and for what purpose? How is the information transmitted?

Information will be shared internally with USDA personnel authorized to access and use this data.

Internal Privacy Impact Analysis

6.2. List the privacy risks and mitigations related to internal information sharing and disclosure. Follow this format:

Privacy Risk: Minimal due to access controls that includes roles that are integrated into the USDA eAuthentication Application.

Mitigation: All access will be managed using the USDA eAuthentication Application.

External Information Sharing

6.3. With which external organizations (outside USDA) is information shared, received, and/or transmitted? What information is shared, received and/or transmitted, and for what purpose? How is the information transmitted?

Information will also be shared, where permitted by law and consistent with this notice, with Federal and State agencies when necessary to investigate and rectify fraudulent or otherwise improper or illegal SNAP enrollments or transactions.

Click or tap here to enter text.

External Privacy Impact Analysis

6.4. List the privacy risks and mitigations related to external information sharing and disclosure. Follow this format:

Privacy Risk: Privacy Act risks associated with sharing information externally include:

- **Unauthorized Access:** Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.
- **Data Breaches:** External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.
- **Loss of Control:** Once PII is shared externally, the SNAP Information Database and USDA may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.
- **Non-compliance with Regulations:** Sharing PII without proper consent or outside the parameters set by privacy laws can result in legal penalties and reputational damage.
- **Inconsistent Data Management Practices:** Different third parties may have varying practices for handling PII, leading to inconsistencies in data protection and increased risks.
- **Insufficient Due Diligence:** Failing to conduct proper due diligence on third parties before sharing PII can expose the SNAP Information Database to risks associated with partnering with unreliable or non-compliant entities.
- **Public Perception and Trust Erosion:** External sharing of PII, especially if not communicated transparently, can lead to public distrust and negative perceptions of the SNAP Information Database or agency.
- **Reputational Damage: I**f shared PII is misused or leads to negative outcomes for individuals, it can result in significant reputational harm to the SNAP Information Database or agency responsible for the data.
- **Limited Individual Awareness:** Individuals may not be fully aware of how their PII is being shared or the potential risks involved, leading to a lack of informed consent.
- **Legal Liability:** The SNAP Information Database and USDA may face lawsuits or legal actions if individuals believe their PII has been mishandled or improperly disclosed, resulting in financial and operational impacts.

Mitigation: Implementing the following mitigation actions, the SNAP Information Database can manage the risk associated with external sharing and disclosure of personal information while complying with Privacy Act requirements.

- **Access Controls:** Implement strict access controls to ensure that only authorized personnel can share or disclose PII externally.

- **Security Measures:** Employ robust security measures, such as encryption and secure transfer protocols, when sharing personal data to protect it during transmission.
- **Data Sharing Policy:** Develop a clear policy outlining the conditions under which PII can be shared externally, including legal and compliance requirements (ex.: Computer Matching Agreements, SORNs, Business Agreements).
- **Due Diligence:** Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.
- **Written Agreements:** Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.
- **Need-to-Know Basis:** Limit the sharing of PII to only what is necessary for the intended purpose, adhering to the principle of data minimization.
- **Individual Consent:** Obtain explicit consent from individuals before sharing their personal information with third parties.
- **Transparency with Individuals:** Clearly inform individuals about potential external sharing of their personal data in privacy notices, including the types of entities with whom data may be shared and the purposes for sharing.
- **Access Controls:** Implement strict access controls to ensure that only authorized personnel can share or disclose PII externally.
- **Individual Consent:** Obtain explicit consent from individuals before sharing their personal information with third parties.
- **Regular Audits:** Conduct regular audits of data sharing practices and third-party compliance to ensure adherence to privacy policies and legal requirements.
- **Incident Response Plan:** Develop an incident response plan that outlines procedures for addressing potential data breaches or unauthorized disclosures related to external sharing.

Section 7: Redress

These questions address the 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?

Data being shared is already provided by individuals to SNAP State agencies for the purpose of determining a household's eligibility for SNAP benefits. Individuals may request data from their State agency who is responsible for collecting and maintaining it.

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

Any individual that receives a notice of adverse action from a State agency that would impact the household's eligibility or benefit allotment has the right to request a fair hearing per the regulations at 7 CFR 273.15. Existing regulations requires State agencies to present all information used to make a decision and provides procedures for the individual to dispute any inaccurate or erroneous information.

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

State agencies must send a notice of adverse action to any individual based on any action by the State agency to reduce or terminate an individual's SNAP benefit based on a data match or any other source of information, per 7 CFR 273.13 of the regulations.

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

Not applicable.

Privacy Impact Analysis

7.5. List the privacy risks and mitigations related to redress. Follow this format:

Privacy Risk: Privacy Act risks associated with redress include:

- **Inadequate Processes:** If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.
- **Lack of Transparency:** Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.
- **Failure to Address Complaints:** The SNAP Information Database or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

- **Delayed Responses:** Slow responses to redress requests can frustrate individuals and exacerbate feelings of mistrust and dissatisfaction, potentially leading to reputational harm.
- **Inconsistent Application:** If redress processes are applied inconsistently across different cases or agencies, it can lead to perceptions of unfairness and bias, undermining trust in the entire department.
- **Insufficient Recordkeeping:** Poor documentation of redress requests and outcomes can hinder an agency's ability to identify patterns of violations, learn from mistakes, and improve practices.
- **Legal Exposure:** Failing to provide adequate redress options may expose the SNAP Information Database or USDA to legal challenges, including lawsuits or regulatory scrutiny, especially if individuals feel their rights have been violated.
- **Reputation Damage:** Public knowledge of inadequate redress mechanisms can damage the department's reputation, leading to loss of customer trust and potential business impacts.
- **Lack of Accountability:** Without effective redress mechanisms, the SNAP Information Database or USDA may not be held accountable for privacy violations, which can perpetuate poor data handling practices.
- **Discrimination:** If redress mechanisms are not accessible to all individuals equally, it may lead to discrimination, where certain groups may find it harder to seek and obtain redress.

Mitigation: To mitigate redress risks, the SNAP Information Database must establish clear, accessible, and effective redress mechanisms, providing transparent information about the process, ensuring timely responses, and maintaining thorough documentation of all complaints and resolutions. Implementing the following mitigation actions, the SNAP Information Database can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

- **Establish Clear Procedures:** Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.
- **User Awareness Campaigns:** Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.
- **Dedicated Point of Contact:** Appoint dedicated personnel who are responsible for handling redress requests and ensuring timely responses to complaints.

- **Timely Response Protocols:** Implement protocols for acknowledging and responding to redress requests promptly, ensuring that individuals feel heard and valued.
- **Investigation Processes:** Create structured process for investigating redress requests, including gathering necessary information and documenting findings.
- **Remediation Options:** Offer various remediation options, such as data correction, deletion, or compensation, depending on the nature of the complaint and the organization's policies.
- **Feedback Mechanisms:** Establish feedback channels for individuals to provide insights on the redress process, helping to improve the system continuously.
- **Regular Training:** Provide ongoing training for employees on handling privacy complaints and the importance of adhering to redress procedures.
- **Monitoring and Reporting:** Regularly monitor redress requests and outcomes to identify trends, potential issues, and areas for improvement in privacy practices.
- **Transparency in Outcomes:** Communicate the outcomes of redress requests to the individuals involved, ensuring transparency and fostering trust in the process.

Section 8: Auditing and Accountability

These questions describe technical safeguards and security measures:

8.1. How is the information in the system/project/program secured?

The SNAP Information Database will be housed within FNS' FedRAMP Amazon Web Services (AWS) environment, and will be protected in accordance with Federal requirements and USDA policy. Identification and authentication are implemented using multi-factor authentication for USDA users through the use of Personal Identity Verification (PIV) smartcards (LincPass). Logical access control to the SNAP Information Database is implemented via USDA eAuthentication Application.

The USDA eAuthentication Application is the system used by USDA agencies to enable FNCS staff, customers, and contractors to obtain accounts that allow them to access USDA web applications and services via the Internet. The USDA eAuthentication Service provides common authentication for web-based applications. Authentication confirms a person's identity, and enables authorization to data and system resources through role-based access controls that identify the person's user system and data permissions.

Data will be encrypted in transit via the MoveIt or Box file transfer application. Once in the SNAP Information Database, security controls and monitoring will be commensurate with USDA, Federal policy, requirements, and FNS' robust and structured information security control and monitoring program. Key features of FNS security program include:

- **Secure Architecture and Configuration:** Security engineers work with application developers and system administrators to ensure that effective security capabilities are implemented appropriately and operating as intended to protect FNS IT resources, in alignment with zero-trust principles. Security capability implementation and validation occur throughout the development process, leveraging FedRAMP cloud solutions, USDA security tools, and FNCS cyber capabilities.
- **Application Security Program:** FNS leverages a proactive approach for identifying, mitigating, and managing vulnerabilities in software applications and supporting platforms through secure coding practices, regular assessment, and continuous improvement. The SNAP Information Database will utilize USDA enterprise vulnerability scanning tools, as well as FNS static code analysis and dynamic application security testing capabilities. Identified vulnerabilities are formally tracked for resolution within mandated remediation timeframes, with regular reports provided to FNS IT and program leadership.

- **Audit Log Management Program:** FNS leverages a centralized strategy and capabilities for collecting, monitoring, and analyzing system and user activity logs to detect anomalies, support incident response, and maintain compliance with regulatory requirements. The SNAP Information Database will generate event logs that will be captured in regular reports and alerts to satisfy regulatory requirements and ensure that suspicious activity is detected, investigated, and addressed as appropriate.
- **Continuous Monitoring:** All FNS systems and applications are subject to a robust continuous monitoring program, to include regular access monitoring and recertification; periodic independent privacy and security assessment; secure configuration and compliance validation; contingency planning and response; and incident management and response.

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

All users of FNS systems must follow the FNS User Access Request process prior to being granted access to a system. Access requests are approved by a supervisor, or contract officer representative (COR) for contractors, and a designated account manager for the system. Access control procedures for the SNAP Information Database will be documented in the system's Access Control (AC) Standard Operating Procedure (SOP).

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

Information sharing requirements will be reviewed before entering into a new sharing agreement. All information sharing agreements are reviewed on an annual basis, in conjunction with the annual security control assessment.

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

All USDA users are required to take annual information security awareness training, which includes elements of privacy-related topics and rules of behavior for accessing USDA systems.

Privacy Impact Assessment Review

Date reviewed by USDA Privacy Office: 7/23/2025

Signed: Signatures on file