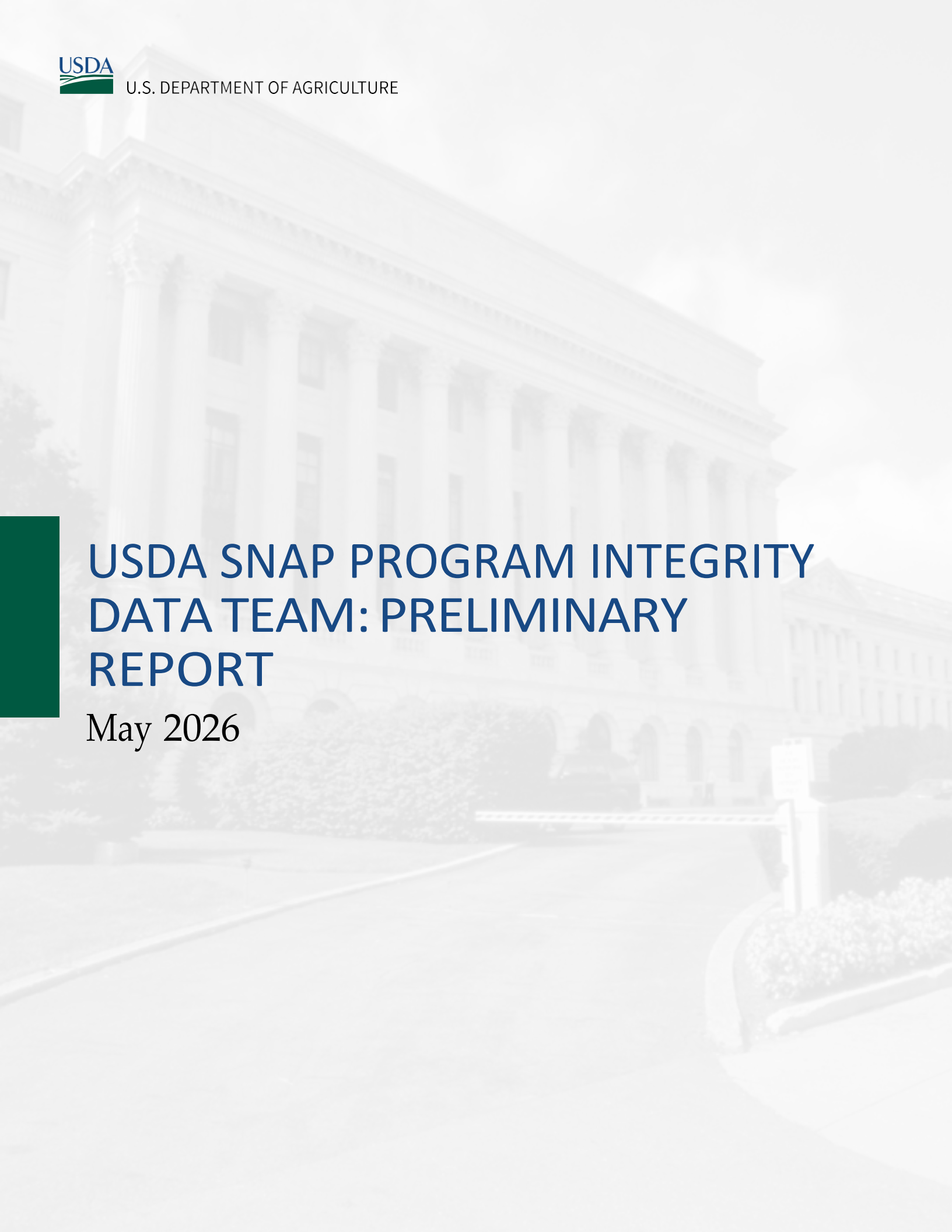

U.S. DEPARTMENT OF AGRICULTURE

USDA SNAP PROGRAM INTEGRITY DATA TEAM: PRELIMINARY REPORT

May 2026

May 13, 2026

The Supplemental Nutrition Assistance Program (SNAP) assists millions of vulnerable Americans each year. It is also a massive taxpayer investment, costing nearly $100 billion per year. Congress tasks the U.S. Department of Agriculture (USDA) with managing that investment and statutorily demands integrity and accountability practices be implemented by both State agencies and USDA. To fulfill that responsibility, USDA will leverage every available tool to prevent fraud and protect the generosity of the American taxpayer.

To that end, in May 2025, Secretary Brooke L. Rollins directed States to share their SNAP eligibility data with USDA, launching a historic and collaborative effort to root out fraud, waste, and abuse. The Department established the first ever SNAP Program Integrity Data Team to analyze the data provided by States and compare it to readily available Federal databases. What they found was alarming; in the data provided by 29 State agencies, initial estimates indicate the team identified at least $3 billion a year of potential fraud, waste, and abuse. This report provides an overview of the team's methodologies and findings.

Today, USDA is working together with these State agencies to verify and, where appropriate, take action on the flags the data analyses revealed. The Trump Administration firmly believes this Federal-State partnership is vital to strengthening SNAP integrity. Together, USDA and States will safeguard SNAP – and American taxpayers – from fraud, waste, and abuse, preserving benefits for those most in need.

Patrick A. Penn
Deputy Under Secretary
Food, Nutrition, and Consumer Services
U.S. Department of Agriculture

Methodology

Introduction

U.S. Department of Agriculture and the Food and Nutrition Service (FNS) use SNAP eligibility data to ensure the integrity of government programs, including by cross referencing SNAP recipient eligibility against federally maintained databases, identifying and eliminating duplicate enrollments, and performing additional eligibility and program integrity checks specified herein. This Standard Operating Procedure (SOP) establishes a framework for State SNAP agencies to share data with the USDA/FNS for fraud, waste, and abuse detection and program integrity purposes. The SOP balances Federal data access requirements under Executive Order 14243 and the Food and Nutrition Act with privacy protections, minimizes unnecessary data collection, and incorporates security standards while maintaining public trust and compliance with applicable law.

Data requested from States

Data requested from States can be found in Appendix A. Only data elements necessary to achieve specific, legally permissible goals, such as fraud detection, duplicate enrollment prevention, and program integrity checks, were collected and used. The scope of data collection was limited to excluding sensitive personally identifying information (PII) unless directly relevant to these goals (i.e., the collection of data elements spelled out in the Privacy Impact Assessment, found in Appendix B). Data derived from third-party sources (employment verification databases, financial institution records, and property records) that States use for verification but are not part of applicant-reported information are excluded and were not requested. The applicable system of records notice for this protocol is USDA/FNS-15, "National Supplemental Nutrition Assistance Program (SNAP) Information Database," as found in Appendix C.

Data transfer and security

The SNAP Information Database's infrastructure and operational procedures were designed to ensure the highest levels of security and compliance. All infrastructure adheres to Federal Risk and Authorization Management Program (FedRAMP) High Baseline standards. Data are encrypted to prevent unauthorized personnel from accessing unencrypted information.

USDA implements role-based access control (RBAC) following the principle of least privilege, with access limited to specifically designated employees and contractors.

All data transfers are conducted using secure tools that meet or exceed FedRAMP High Baseline standards, ensuring the integrity and security of the data throughout the transfer process.

Processing

States store and organize their data very differently, so State-specific processing procedures were developed to rapidly read in and synchronize data across all States when received. Special attention was paid to coordinating date fields, ensuring true recipients' data were in fact active participants in SNAP, and removing duplication. Some States provided multiple instances of a given recipient when their data were updated (i.e. address change), and care

was taken to ensure current information was being considered. Data were arranged into tidy format, such that a single row per active recipient and a single column per category of data were created. States were consulted during this process to ensure proper interpretation of data formats and column definitions.

Flagging State data

USDA employed a foundational fraud, waste, and abuse verification that focused on identity verification, income and eligibility verification, immigration status, reported residential and mailing addresses, verification of disqualified recipients, as well as non-recipient household member data. USDA cross referenced State supplied data against auxiliary data from other sources including Social Security Administration (SSA), Systematic Alien Verification for Entitlements (SAVE), and other internal FNS data sources to establish data integrity. Date of birth, household size, and spending patterns were used to glean insight on income and eligibility verification. No official flag or determination was made with regard to income, but spending patterns were linked to eligibility data from internal FNS data sources. SSA data coupled with SAVE data were used to flag possible immigration status discrepancies. The FNS Electronic Disqualification Recipient System was used to flag recipient disqualification status.

In addition to the core fraud detection functions, USDA employed additional techniques including flagging intrastate and interstate duplication, deceased individuals, synthetic identity patterns (new social security numbers [SSNs] with inconsistent biographical data), and geographic anomalies (such as high out-of-state transactions). Intrastate and interstate duplication flags were raised on individual social security numbers that were duplicated within (intrastate) or between states (interstate). Deceased individuals and synthetic identity patterns were flagged based on links with SSA data and consistency within State active eligibility data (i.e. same names and birth dates assigned to different SSNs, heads of household with unrealistic birthdates, or data that fit typical dummy-data patterns, such as SSNs of 123-45-6789 or similar configurations).

Reporting to States

After analysis, identified data discrepancy flags were returned to some of the State agencies with a summary of all flag counts by zip code and an identified category tab for each of the flags described above. States were asked to review a sample of each flag in each of the respective categories and provide feedback on the efficacy of the flagging procedure. States were encouraged to provide final disposition of each case review. USDA personnel will use feedback to improve initial data read in or State-specific flagging or output procedures.

Exclusions

Data was not used for tax administration or tax compliance, immigration enforcement, law enforcement investigations beyond coordination regarding criminal and administrative SNAP violations, administration of non-SNAP federal assistance programs (e.g., Medicaid, Temporary Assistance for Needy Families, housing assistance), sharing with foreign governments or international organizations, commercial use or transfer to private entities, or determining federal eligibility for benefits other than SNAP.

Table 1: SNAP Participation and Data Supplied by State Agency

State / Territory	SNAP Participation June 2025[1]	Responded to Data Request?
Alabama	732,974	YES
Alaska	66,572	YES
Arizona	886,806	NO
Arkansas	241,210	YES
California	5,477,070	NO
Colorado	614,911	NO
Connecticut	361,655	NO
Delaware	118,766	NO
District of Columbia	140,716	NO
Florida	2,928,850	YES
Georgia	1,385,834	YES
Guam	39,285	YES[2]
Hawaii	149,284	NO
Idaho	132,534	YES
Illinois	1,869,744	NO
Indiana	580,902	YES
Iowa	266,947	YES
Kansas	186,560	NO
Kentucky	593,934	NO
Louisiana	791,032	YES
Maine	163,056	NO
Maryland	665,084	NO
Massachusetts	1,079,234	NO
Michigan	1,474,701	NO
Minnesota	448,841	NO
Mississippi	356,756	YES
Missouri	660,033	YES
Montana	80,066	YES
Nebraska	149,699	YES
Nevada	492,270	YES
New Hampshire	75,489	YES
New Jersey	821,038	NO
New Mexico	458,019	NO
New York	2,955,731	NO
North Carolina	1,350,026	YES
North Dakota	51,179	YES
Ohio	1,437,112	YES
Oklahoma	691,754	YES

State / Territory	SNAP Participation June 2025[1]	Responded to Data Request?
Oregon	772,310	NO
Pennsylvania	1,941,067	NO
Rhode Island	141,801	NO
South Carolina	570,687	YES
South Dakota	75,329	YES
Tennessee	682,128	YES
Texas	3,457,259	YES
Utah	174,386	YES
Vermont	64,094	YES
Virginia	813,228	YES
Virgin Islands	20,610	NOT REQUIRED
Washington	903,442	NO
West Virginia	269,687	YES
Wisconsin	687,133	NO
Wyoming	26,927	YES
TOTAL	**41,575,762**	

[1] Preliminary data as of September 2025.
[2] Guam was not required to provide data but voluntarily responded to the request.

Findings

Table 2: SNAP Eligibility Data Discrepancies for 29 State Agencies – Data as of July 1, 2025

Issue	Total Count 29 State Agencies	Median State Count[1]	Median State Percent[2]	Annual Implied Dollars[3]
Intrastate Duplication	247,575	467	0.10%	558,529,200
Interstate Duplication	108,670	2,057	0.50%	245,159,520
Deceased (per SSA record)	185,986	2,005	0.60%	419,584,416
Dummy SSN	441,572	2,462	1.20%	996,186,432
No SSN Found	26,333	254	0.10%	59,407,248
Disqualified but Active	4,442	56	0.03%	10,021,152

[1] Median count of each item for 29 State agencies supplying data.
[2] Median percent of records per state for each item in 29 State agencies supplying data.
[3] Calculated as $2256 per recipient annually ($188 per month).

Intrastate Duplication: Recipients with same identifiers (SSN) that show up multiple times within a State.

Interstate Duplication: Recipients with same identifiers (SSN) that show up in multiple States.

Deceased (per SSA Record): Based on SSA lookup, the recipient is deceased.

Dummy SSN: Recipient has a non-normal SSN (i.e. 111-11-1111 or 999-99-9999).

No SSN Found: Recipient does not have an SSN in data provided.

Disqualified but Active: Recipient has been identified as a disqualified participant but is still active on State agency rolls.

Data Summary

The review of SNAP eligibility data across 29 State agencies identified several categories of discrepancies that could signal improper or erroneous benefit issuance. The largest issues by volume were cases with dummy or missing SSNs and intrastate duplication, together representing hundreds of thousands of records. Interstate duplication and deceased individuals appearing as active participants also showed substantial counts. Although the median percentage of each issue within States appear small, general under 1.2%, the implied annual financial exposure is significant. Dummy SSNs and intrastate duplication together account for more than $1.5 billion in estimated annual risk. Overall, the findings indicate that even small error rates can translate into substantial fiscal impact when applied across large caseloads, underscoring the importance of strengthened data-matching and eligibility verification controls.

These results highlight the need for targeted oversight, improved data integrity efforts, and sustained collaboration with States to reduce vulnerabilities and ensure program accuracy.

Appendix A

Supplemental Nutrition Assistance Program

Information SNAP Database

SNAP Eligibility Data Elements

The following elements should be included in the data sharing file from each State agency on all household members that are listed in the SNAP case. Please provide a data dictionary if one is available to reduce the burden to both the State agency and USDA.

Case Number: The case number is a unique identifier, typically 7 to 10 digits long, assigned to a household when they apply and/or are approved for SNAP.

First, Middle, Last Names: The full name of all household members.

Known Alias: Assumed or alternative name(s) used by any of the household members.

Authorized Representative(s): Provide any identified authorized representative for the household, and their corresponding information such as full name, means of verbal and written communication.

Date of Birth: The specific month, day and year the household member was born.

Individual Recipient Identification Number: The unique identifier assigned to that specific household member within the case by the State agency.

Social Security Number: The unique 9-digit identifier issued by the Social Security Administration and provided by the household member.

Status on SNAP (recipient/individual level): Identify if the household member in the case is actively receiving SNAP, disqualified, sanctioned, or excluded.

Application and/or Recertification Date: The date the household applied for SNAP (this can be the first application date, or most recent recertification date).

Reporting Status: Following initial certification, or recertification, households are determined to be a simplified or change reporting household. This data element should indicate the reporting status the household has been designated to be.

Relationship: The relationship identifies who all household group members are to one another and assists with determining mandatory group members. The data should reflect who each household member is to one another.

Absent Parent (as applicable): This identifies the parent of a minor child who resides in a separate household.

Citizenship and/or Immigration Status: This identifies if the individual is a U.S. citizen or immigrant. The status should be available in the data elements to be matched against SAVE and/or SSA for verification. Please provide any known or reported enumerator numbers for all household members.

Residential Address: The address the household has provided as to where they reside.

Mailing Address: The address the household has provided as to where they would like all correspondence sent to (if different than residential).

Homeless Status: Please include if the household is identified as homeless.

Phone Number(s): The contact number(s) provided by the household as a means of contact.

Email Address(es): The email address(es) provided by the household as a means of contact.

Unearned Income: The unearned income (RSDI, unemployment, child support, etc.) identifies the unearned income source, pay frequency, the household member receiving the pay, and the total amount of income budgeted to determine the SNAP allotment.

Earned Income: The earned income identifies the earned income source, pay frequency, the household member receiving the pay, and the total amount of income budgeted to determine the SNAP allotment.

Self-Employment Income: Self-employment should be identified as to what the self-employment is (type or business name), pay frequency, the household member who is self-employed, and the total amount of income budgeted as well as the amount of allowed expenses.

Shelter Expenses: The shelter expenses should be identified as to shelter type (i.e. rent), and the budgeted dollar amount. Shelter expenses may be separated out as various expenses are taken into consideration for eligibility and those should be included if used in the SNAP allotment determination (i.e. telephone, heating, cooling). If the household is active with Section 8, which pays a portion of the rental expenses, please ensure that is included.

Assets/Resources: Any known assets (i.e. bank accounts, boat, collector vehicle) or resources used to determine SNAP eligibility and must identify the asset type, amount and what household member the asset belongs to.

Sanctions/Disqualifications: Identify any household members who are serving a sanction and/or disqualification that is impacting their eligibility to participate in SNAP. The sanction and/or disqualification type and any applicable time periods should be identified (i.e. IPV, 10/1/2024-9/30/2025). This field should correspond to the data provided in the status on SNAP if the household member is currently serving a disqualification, as well as any income field(s) that may pertain to the disqualified member due to income proration.

SNAP EBT Card Number: The unique set of digits on the household's issued SNAP EBT card that connects the case to the associated transactions. This data helps the USDA pull all respective transactions related to the household.

Appendix B

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
☐ Dental Profile
☐ Eye Color
☐ Photos
☐ Signatures

Characteristics

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

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

Appendix C

Notices

Federal Register
Vol. 90, No. 118

Monday, June 23, 2025

This section of the FEDERAL REGISTER contains documents other than rules or proposed rules that are applicable to the public. Notices of hearings and investigations, committee meetings, agency decisions and rulings, delegations of authority, filing of petitions and applications and agency statements of organization and functions are examples of documents appearing in this section.

DEPARTMENT OF AGRICULTURE

Privacy Act of 1974; System of Records

AGENCY: Department of Agriculture (USDA), Food and Nutrition Service (FNS).

ACTION: Notice of a new system of records.

SUMMARY: Pursuant to the provisions of the Privacy Act of 1974 and Office of Management and Budget (OMB) Circular No. A–108, notice is hereby given that the United States Department of Agriculture (USDA) proposes to create a new system of records (SOR) entitled USDA/FNS–15, ''National Supplemental Nutrition Assistance Program (SNAP) Information Database.'' This system is owned, administered, and secured by the Food and Nutrition Service (FNS). The primary purposes of this system are to validate the accuracy of eligibility determinations and strengthen SNAP and government program integrity.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this system of records notice will become effective upon publication in the **Federal Register**, except for the routine uses, which will become effective on July 23, 2025, unless USDA determines they must be changed as a result of public comment. USDA will publish any changes to the system of records notice resulting from public comment.

ADDRESSES: Interested parties may submit written comments by one of the following methods:

- *Preferred:* Federal eRulemaking Portal at *http://www.regulations.gov* provides the ability to type short comments directly into the comment field on this web page or attach a file for lengthier comments. Follow the online instructions at that site for submitting comments.
- *By email:* [Insert email contact]
- *By mail:* [Insert mail contact], FNS, 1320 Braddock Place, Alexandria, VA 22314.

Instructions: All comment submissions must include the agency name and docket number for this rulemaking. All comments received will be posted without change to *http://www.regulations.gov,* including any personal information provided. However, comments containing profanity or inappropriate or abusive content may be rejected or redacted before posting.

Docket: For access to the docket to read background documents or comments received go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: FNS Privacy Officer, Information Management Branch, Food and Nutrition Service, USDA, 1320 Braddock Pl, Alexandria, Virginia 22314; or via email at *SM.fn.Privacy-FNS@usda.gov.*

SUPPLEMENTARY INFORMATION:

Background

Pursuant to, among other authorities, 7 U.S.C. 2020(a)(3) and (e)(8)(A) and 7 CFR 272.1(c)(1) and (e), FNS will work with all State agencies and their designated vendors and/or contractors to transmit data on SNAP participants and transactions for the purposes listed below. This system is consistent with and effectuates multiple executive orders, including but not limited to Executive Order 14243 of March 20, 2025, *Stopping Waste, Fraud, and Abuse by Eliminating Information Silos* and Executive Order 14218 of February 19, 2025, *Ending Taxpayer Subsidization of Open Borders.*

USDA and FNS will use the SNAP data in this system to ensure the integrity of Government programs, including by verifying SNAP recipient eligibility against federally maintained databases, identifying and eliminating duplicate enrollments, and performing additional eligibility and program integrity checks specified herein.

The system of records notice explains how the records within the new system will be used and with whom they will be shared.

Privacy Act

The Privacy Act of 1974 (the Privacy Act), 5 U.S.C. 552a, embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates records about individuals. The Privacy Act applies to information that is maintained in a SOR. A SOR is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and lawful permanent residents.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each SOR that the agency maintains, to publish the routine uses that are contained in each system in order to make agency record keeping practices transparent, and to notify individuals regarding the uses and locations of their records.

In accordance with 5 U.S.C. 552a(r), USDA has provided a report of this SOR to the Office of Management and Budget and to the relevant committees of Congress.

SYSTEM NAME AND NUMBER:

USDA/FNS–15, National SNAP Information Database.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The National SNAP Information Database is maintained in the FNS Amazon Web Service (AWS) cloud infrastructure environment that is used only by Federal employees and contractors. The data is processed and stored solely within the continental United States. The agency, U.S. Department of Agriculture, address is 1400 Independence Ave. SW, Washington, DC 20250 and the address of the third-party service provider is Microsoft, 1 Microsoft Way, Redmond, Washington 98052–6399.

SYSTEM MANAGER(S):

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

7 U.S.C. 2020(a)(3) and (e)(8)(A); 7 CFR 272.1(c)(1) and (e); Executive Order (E.O.) 14243; Executive Order 14218.

PURPOSE(S) OF THE SYSTEM:

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.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who have received, are currently receiving, or have applied to receive SNAP benefits.

CATEGORIES OF RECORDS IN THE SYSTEM:

The system consists of records containing personally identifying information, including but not limited to SNAP participant name, Social Security Number (SSN), date of birth (DOB), residential address, Electronic Benefit Transaction (EBT) card number, and case record identifier number or other identifiers or data elements maintained by States, vendors, or contractors to identify SNAP recipients. The system also consists of information derived from and associated with EBT transactions, including but not limited to records sufficient to calculate the total dollar value of SNAP benefits received by participants over time, such as applied amounts and benefit available dates.

RECORD SOURCE CATEGORIES:

Information in this system is provided by the 53 State agencies that administer SNAP and their designated vendors and/or contractors. Information in this system is also provided by other Federal agencies with which USDA partners on program integrity efforts.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

Records created or stored in this system may be disclosed pursuant to the permitted routine uses outlined below to the extent such uses are authorized by, among other authorities, 7 U.S.C. 2020(a)(3) and (e)(8), 7 CFR 272.1(c)(1) and (e), and Executive Orders 14218 and 14243.

(1) To the Department of Justice or in a proceeding before a court or adjudicative body when: (a) USDA/FNS or any component thereof; or (b) any employee of USDA in his or her official capacity, or any employee of the agency in his or her individual capacity where the Department of Justice has agreed to represent the employee; or (c) the United States Government, is a party to litigation or has an interest in such litigation, and USDA determines that the records are both relevant and necessary to the litigation and the use of such records by the Department of Justice is deemed by USDA to be for a purpose that is compatible with the purpose for which USDA collected the records.

(2) In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the USDA/FNS or other Agency representing the USDA, determines that the records are both relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant and necessary to the proceeding.

(3) To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the request of, and on behalf of, the individual about whom the record is maintained.

(4) To the National Archives and Records Administration or other Federal government agencies pursuant to records management activities being conducted under 44 U.S.C. 2904 and 2906.

(5) To another Federal agency or Federal entity, when USDA/FNS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in: (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

(6) To appropriate agencies, entities, and persons when: (1) USDA/FNS suspects or has confirmed that there has been a breach of the system of records; (2) USDA/FNS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, USDA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with USDA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

(7) To contractors, grantees, experts, consultants, and the agents thereof, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for USDA, when necessary to accomplish an agency function related to this system of records. USDA and FNS will require individuals provided information under this routine use to comply with all applicable requirements and limitations of disclosure imposed by the Privacy Act.

(8) When a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, USDA/FNS may disclose the record to the appropriate agency, whether Federal, foreign, State, local, or tribal, or other public authority responsible for enforcing, investigating, or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutive responsibility of the receiving entity.

(9) To Federal and State Agencies responsible for: (1) the administration of SNAP; or (2) the administration of other Federal benefits programs to the extent permitted by applicable law when such information is necessary for the performance of lawful audit, oversight, or administrative functions.

(10) To the U.S. Department of the Treasury when disclosure of the information is relevant and necessary to review payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds, including funds disbursed by a state (meaning a state of the United States, the District of

Columbia, a territory or possession of the United States, or a federally recognized Indian tribe) in a state-administered, federally funded program.

(11) To support another Federal agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States (including any State or local governmental agency), that administers, or that has the authority to investigate or assist USDA to investigate potential fraud, waste, or abuse in, a Federal benefits program funded in whole or in part by Federal funds, when disclosure is deemed reasonably necessary by USDA to prevent, deter, discover, detect, investigate, examine, prosecute, sue with respect to, defend against, correct, remedy, or otherwise combat fraud, waste, or abuse in such programs.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

The National SNAP Information Database will be hosted in the FNS AWS Cloud infrastructure environment, which is FedRAMP certified. These records are electronic.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be indexed and retrieved by the name of the individual, SSN, EBT card number, case record identifier number, or any other identifier or data element used by any State, vendor, or contractor to identify SNAP recipients.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

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. 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.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

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

Technical Safeguards: The National SNAP Information Database will utilize a robust collection of technical safeguards to ensure the integrity of the platform. The National SNAP Information Database is designed to meet all technical safeguards required by its system categorization in National Institute of Standards and Technology (NIST) 800–53. The National SNAP Information Database will be hosted in a secure environment that uses perimeter security protection to prevent interference or access from outside intruders. When accessing the National SNAP Information Database, Secure Socket Layer (SSL)/Transport Layer Security (TLS) technology protects the user's information by using both server authentication and data encryption. Users will only access the National SNAP Information Database by USDA eAuthentication through Personal Identity Verification (PIV) Card and Personal Identification Number (PIN) entry or Login.gov. The National SNAP Information Database administrators will have a suite of security tools that can be used to increase the security of the system.

Physical Safeguards: The servers that host the National SNAP Information Database are stored in a USDA FedRAMP authorized data center with strict physical access control procedures in place to prevent unauthorized access.

RECORD ACCESS PROCEDURES:

Personal information contained in this system is provided by the State agency, or such agency's designated vendors and/or contractors, in the State where the individual is a SNAP participant or applicant. An individual may obtain information about a record in the system which pertains to the individual by submitting a written request to the systems manager listed above via letter or online at *https://efoia-pal.usda.gov/.* If by mail, the letter should be marked ''Privacy Act Request.'' Requests should include the name of the individual making the request, the name of the system of records, any other information specified in the system notice, and a statement of whether the requester desires to be supplied with copies by mail or electronically. Individuals may also directly contact the applicable State agency or local SNAP office. A request for information pertaining to an individual should contain the name, address, date of birth, and SSN of the individual, and any other information that will assist in locating the record.

CONTESTING RECORD PROCEDURES:

Individuals desiring to contest or amend information maintained in the system should direct their request to the system manager listed above or to the State agency or designated vendor/contractor that provided the data. The request should identify each 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. Where consistent with the Privacy Act and this notice, requests sent to the system manager will be shared with the State agency in the State where the individual is a SNAP participant or applicant for resolution. Requests must follow the procedures set forth in 7 CFR 1.116 (Request for correction or amendment to record).

NOTIFICATION PROCEDURES:

Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to the individual, from the System Manager listed above: See RECORD ACCESS PROCEDURES.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

James C. Miller,

Administrator.

[FR Doc. 2025–11463 Filed 6–20–25; 8:45 am]
BILLING CODE 3410–30–P

CIVIL RIGHTS COLD CASE RECORDS REVIEW BOARD

[Agency Docket Number: CRCCRRB–2025–0017–N]

Notice of Formal Determination on Records Release

AGENCY: Civil Rights Cold Case Records Review Board.

ACTION: Notice.

SUMMARY: The Civil Rights Cold Case Records Review Board received 4,701 pages of records from the National Archives and Records Administration (NARA), the Department of Justice, and the Federal Bureau of Investigation (FBI) related to five civil rights cold case incidents to which the Review Board assigned the unique identifiers 2023–