U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

Privacy Impact Assessment

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement, PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:



Civil Rights Document Routing (CRDR)

Supplemental Nutrition Assistance Program (SNAP)

Food Nutrition and Consumer Services

Date PIA submitted for review:

April 30, 2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Deea Coleman	Deea.Coleman@usda.gov	Not listed
Information System Security Manager	John Rosselot, Jr.	John.Rosselotjr@usda.gov	571-563-5260
System/Program Managers	James Bosse	James.Bosse@usda.gov	703-605-0572

Abstract

The abstract provides the simplest explanation for the "what does the system do?" and will be published online to accompany the PIA link.

The Civil Rights Document Routing (CRDR) application supports the Food, Nutrition and Consumer Services (FNCS) Supplemental Nutrition Assistance Program (SNAP). The purpose of the application is to provide a means to review and route documents to FNCS, region or state stakeholders that have been erroneously sent to the USDA's Office of the Assistant Secretary for Civil Rights (OASCR). The FNCS Civil Rights Division (CRD) redistributes the documents among the four FNCS programs: SNAP), Child Nutrition Programs (CNP), Food Delivery Distribution Division (FDD), and Women Infants and Children (WIC). Once documents are received by SNAP, the documents are routed to the regions for quality assurance review before they are grouped by state for access by the various external state users. The documents consist of benefit applications, complaints, referrals, verifications, fair hearing requests, periodic reports, and other miscellaneous data. Most of these documents contain personally identifiable information (PII); as such, a Privacy Impact Assessment (PIA) is required.

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 Civil Rights Document Routing (CRDR) application supports the Food, Nutrition and Consumer Services (FNCS) Supplemental Nutrition Assistance Program (SNAP). The purpose of the application is to provide a means to route documents to FNCS, region or state stakeholders that have been erroneously sent to the USDA's Office of the Assistant Secretary for Civil Rights (OASCR). The FNCS Civil Rights Division (CRD) redistributes the documents among the four FNCS programs: SNAP), Child Nutrition Programs (CNP), Food Delivery Distribution Division (FDD), and Women Infants and Children (WIC). Once documents are received by FNCS the documents are routed to the regions for quality assurance review before they are grouped by state for access by the various external state users. The documents consist of benefit applications, complaints, referrals, verifications, fair hearing requests, periodic reports, and other miscellaneous data.

The application routes documents in the system until they eventually achieve one of the following statuses: *returned*, *archived*, *downloaded* or *deleted*.

The CRDR application is downstream from the collection process and the primary purpose of the system is to move the misdirected mail, in the form of benefit applications, from FNCS Civil Rights and to help FNCS SNAP forward the misdirected mail to the states/territories that need to process the benefit applications.

This solution falls under the aegis of the Food Nutrition Act of 2008, in regard to its handling of files which contain Personally Identifiable Information (PII). Updates to the solution shall be made as directed due to applicable legal and regulatory changes that may occur.

Section 1.0 Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

The Food Nutrition Act of 2008 serves as the basis for legal authority for the application's handling of files which may contain PII.

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

There are two (2) authorizations to operate (ATO) boundaries associated with this application. The application itself resides in the USDA O-365 ATO boundary with a single database to support CRDR residing in the FNCS managed Microsoft Azure cloud for enterprise level supporting components. The corresponding FNCS ATO boundary is the FNS Infrastructure General Support System (FNS I-GSS) which was last authorized 02/08/2023 with an expiration date of 02/08/2026.

USDA is responsible for the ATO of Microsoft O-365. Please refer to USDA for more information regarding the A&A dates for Microsoft O-365.



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

USDA/FNS-9, (formerly known as USDA/FCS-9), Food Stamp Program Retailer Information - 64 FR 17604 - April 12, 1999.

USDA/FNS-12 Food and Nutrition Service (FNS), Women, Infants, and Children (WIC) Food Delivery Portal (FDP) - 86 FR 55803 - October 7, 2002.

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

Yes. SNAP applications are covered under the Paperwork Reduction Act. The Office of Management and Budget (OMB) Control number is 0584-0064.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers						
\boxtimes	Social Security number	\boxtimes	Truncated or Partial Social Security number			
\boxtimes	Driver's License Number		License Plate Number			
	Registration Number	\boxtimes	File/Case ID Number			
\boxtimes	Student ID Number	\boxtimes	Federal Student Aid Number			
\boxtimes	Passport number	\boxtimes	Alien Registration Number			
	DOD ID Number		DOD Benefits Number			
\boxtimes	Employee Identification Number		Professional License Number			
\boxtimes	Taxpayer Identification Number	\boxtimes	Business Taxpayer Identification Number (sole proprietor)			
\boxtimes	Credit/Debit Card Number	\boxtimes	Business Credit Card Number (sole proprietor)			
	Vehicle Identification Number		Business Vehicle Identification Number (sole proprietor)			
\boxtimes	Personal Bank Account Number	\boxtimes	Business Bank Account Number (sole proprietor)			
	Personal Device Identifiers or Serial Numbers		Business device identifiers or serial numbers			



					(sole pr	oprietor)	
\boxtimes	Personal Mobile Number		\boxtimes	Business Mobile Number (sole proprietor)			
\boxtimes	Health Plan Beneficiary Number				I		
Biographical Information							
\boxtimes	Name (including nicknames)	\boxtimes	Sex	\boxtimes	Busines	ss Mailing Address (sole proprietor)	
\boxtimes	Date of Birth (MM/DD/YY)	\boxtimes	Ethnicity	\boxtimes	Busines	ss Phone or Fax Number (sole proprietor)	
\boxtimes	Country of Birth	\boxtimes	City or County of Birth		Group/	Organization Membership	
\boxtimes	Citizenship	\boxtimes	Immigration Status	\boxtimes	Religio	n/Religious Preference	
\boxtimes	Home Address	\boxtimes	Zip Code	\boxtimes	Home I	Phone or Fax Number	
\boxtimes	Spouse Information	\boxtimes		\boxtimes	Children Information		
\boxtimes	Marital Status	\boxtimes	Military Service Information	\boxtimes	Mother's Maiden Name		
\boxtimes	Race	\boxtimes	Nationality		Global Positioning System (GPS)/Location Data		
\boxtimes	Personal e-mail address	\boxtimes	Business e-mail address	\boxtimes	Personal Financial Information (including loan information)		
\boxtimes	Employment Information		Alias (username/screenn ame)		Business Financial Information (including loan information)		
\boxtimes	Education Information		Resume or curriculum vitae		Professional/personal references		
Biometrics/Distinguishing Features/Characteristics							
	Fingerprints		Palm prints		Vascula	r scans	
	Retina/Iris Scans		Dental Profile		Scars, r	narks, tattoos	
	Hair Color		Eye Color		Height		
	Video recording		Photos		Voice/ Audio Recording		
	DNA Sample or Profile		Signatures		Weight		
Medical/Emergency Information							
\boxtimes	Medical/Health Information		Mental Health Information			Disability Information	
\boxtimes	Workers' Compensation Information		Patient ID Number			Emergency Contact Information	
Device Information							



	Device settings or preferences (e.g., security level, sharing options, ringtones)		Cell tower records (e.g., logs, user location, time, etc.)		Network communications data	
Specific Information/File Types						
\boxtimes	Personnel Files	\boxtimes	Law Enforcement Information		Credit History Information	
\boxtimes	Health Information		Academic/Professional Background Information		Civil/Criminal History Information/Police Record	
\boxtimes	Case files		Security Clearance/Background Check	\boxtimes	Taxpayer Information/Tax Return Information	

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

The documents processed in the system are placed into the system by users internal to the USDA from the Office of the Assistant Secretary for Civil Rights (OASCR).

2.2.1. How is the information collected?

OASCR receives documents from external entities, at will, and scans them into CRDR.

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

Not applicable. The CRDR application does not utilize third-party data.

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

The CRDR application will not review the document contents for completeness nor accuracy. The CRDR application will use routing rules based on unique criteria related to the various business units in an attempt to route documents to their proper destinations.

2.5. Does the system/program use third-party websites?

No

Privacy Impact Assessment

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 through the use of third-party websites?

Not applicable.

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

Follow the format below:

Privacy Risk: There is a risk that the information could be used for malevolent purposes.

<u>Mitigation</u>: The CRDR application is only made available to FNCS personnel. The FNCS personnel have to go through an approval and profile setup process to access the information. The information in the CRDR application is safe due to the fact that the system is behind the FNCS firewall and is not accessible to the public. The FNCS personnel will leverage the system to deliver information to the states/territories for processing.

Section 3.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

All information in the CRDR application will be specific to the processing of the documents and not directly related to the document contents. The information tracked in the application will be for the following purposes.

- Loading documents for routing.
- Status tracking for documents.
- Document routing.
- Document review and validation; and
- Staging documents for download.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

The CRDR application has reporting features to provide the application's users with views into the following aspects:

- Processing time from upload to final routing destination.
- Details by SNAP Regions.

Privacy Impact Assessment

- Details by SNAP States; and
- Details by document volume.

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

Follow the format below:

Privacy Risk: There is a risk that the information could be used for malevolent purposes.

<u>Mitigation</u>: The CRDR application is only made available to FNCS personnel, and all components utilize USDA's eAuthentication. The FNCS personnel go through an approval and profile setup process in order to access the information. The information in the CRDR application is safe due to the fact that the system is behind the FNCS firewall and is not accessible to the public. The FNCS personnel will leverage the system to deliver information to the states/territories for processing.

Section 4.0 Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to use of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

Notice is outside the scope of the CRDR; the application does not collect information from individuals. The purpose of the application is for routing misdirected mail.

4.2. What options are available for individuals to consent, decline, or opt out of the project? Not applicable. CRDR does not collect information from individuals. It is a tool to route misdirected communications within the agency.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

Privacy Risk: Notice to benefit applicants is out of scope for the CRDR application.

Mitigation: Not applicable

Section 5.0 Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

5.1. What information is retained and for how long?



Information is retained in a USDA maintained M365 library; it is not retained within FNCS' ATO boundary. Within this context, data retention is out of scope for CRDR.

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

Information is retained in a USDA maintained M365 library; it is not retained within FNCS' ATO boundary. Within this context, data retention is out of scope for CRDR.

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 6.0 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

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

Documents in the CRDR application are shared between the following FNCS program areas based on automated routing or manual routing by application users.

- The Office of the Assistant Secretary for Civil Rights.
- Civil Rights Division.
- Child Nutrition Programs.
- Food Delivery Distribution Division.
- Supplemental Nutrition Assistance Program; and
- Women Infants and Children (WIC).

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

Follow the format below:

Privacy Risk: There is a risk that benefit applications can be routed to an incorrect program area.

<u>Mitigation</u>: Misdirected benefit applications between the program area folders within the CRDR application is an accepted risk. The CRDR application has the functionality where the application's users

Privacy Impact Assessment

can send misdirected files back to OASCR and/or CRD. Once returned, the CRD personnel can re-direct the previously misdirected file to its correct program area folder for processing.

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

For SNAP documents, once documents have been validated by the users that represent a SNAP Region, those documents are shared with their counterparts at the appropriate state/territory for processing. The documents can be transmitted in one of the following ways:

- Email
- SharePoint access via eAuthorization
- File Transfer Protocol (FTP)

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

Follow the format below:

<u>Privacy Risk</u>: There is a risk that SNAP documents could be misdirected between SNAP regions or even SNAP states.

<u>Mitigation</u>: Misdirected SNAP documents between the SNAP region and SNAP state folders within the CRDR application is an accepted risk. The CRDR application has the functionality where SNAP regional users can send misdirected files back to "SNAP Region QA Pending" or "SNAP Pending State Action". Once returned, the SNAP regional users can re-direct the previously misdirected file to its correct region or state folder for processing.

Section 7.0 Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1. What are the procedures that allow individuals to gain access to their information?

Redress is outside the scope of the CRDR application, but notification is provided by the program area and the states/territories. Information notices are labeled on the forms, associated documentation and websites.

Benefit applicants will not be able to access their documents within the CRDR system. The CRDR system is only available to FNCS personnel within the following Program Areas; Civil Rights Division (CRD), Child Nutrition Program (CNP), Food Distribution Division (FDD), Supplemental Nutrition Assistance Program (SNAP) and Women Infants and Children (WIC).

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

Correction of inaccurate or erroneous information on documents are outside the scope of the CRDR application. If the information is incorrect, the state agency will need to communicate with the benefit



applicant. The core purpose of the CRDR application is to route misdirected mail to the correct location (state/territory).

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

Procedural notification is outside the scope of the CRDR system; the CRDR only reroutes misdirected communications to the correct office.

7.4. If no formal redress is provided, what alternatives are available to the individual? Redress is outside the scope of the CRDR application.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk: Redress from benefit applicants is out of scope for the CRDR application.

Mitigation: Not applicable.

Section 8 Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.

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

Any approved USDA account holder will be eligible to access the system. Direct access to the CRDR system will have to be approved by the System Owner, which requires establishing a profile within the application and coordinating with Client Experience Center (CEC) to attach a unique license to the potential User's Active Directory (AD) account. The CRDR application encrypts the data held within, the system produces metadata, which is used to produce a log of User activity within the system.

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

FNCS users for the CRDR component covered under this PIA must submit two FNS-674 forms: one is for the Azure Subscription that is approved by an Account Manager, and a second which functions to provision Azure SQL Database access. The latter form is approved by the OIT Program Management Branch Chief.

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

The objective of the SNAP Program regarding the CRDR system is to identify and re-direct misdirected mail to the intended recipient. In many cases the intended recipients are counterparts of the SNAP National Office at the various states/territories. To aid in this endeavor the SNAP Program defers to FNCS policies and protocols. Information sharing agreements will fall under the approach advised under NIST SP800-47 Rev. 1 and for system access internal users are subject to FNS-674 and external users are subject to the eAuthentication process.