U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

Food Nutrition and Consumer Services (FNCS)

Financial Management System (FNCS FMS)

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

Privacy Impact Assessment: FNCS FMS

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

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

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

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

Privacy Impact Assessment: FNCS FMS

Privacy Impact Assessment for the USDA IT System/Project:

Financial Management System (FMS)

Food and Nutrition Consumer Services (FNCS)

Date PIA submitted for review:
10/15/2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Deea Coleman FNCS Privacy Officer	Deea.Coleman@usda.gov	unlisted
Information System Security Manager	John Rosselot Chief, Risk Management Branch	John.Rosselotjr@usda.gov	571-563-5260
System/Program Managers	Erin McBride	Erin.McBridel@usda.gov	703-305-2709

Privacy Impact Assessment: FNCS FMS

Abstract

This Privacy Impact Assessment (PIA) is for the FNS Financial Management System (FNCS FMS). FNCS FMS includes financial applications and supporting platforms, hosted within the Microsoft (MS) Azure FedRAMP cloud environment, that the Food, Nutrition, and Consumer Service (FNCS) leverages to gather, process, and report on financial data.

Overview

The FNCS FMS includes the financial applications and supporting platforms, which are hosted within the Microsoft (MS) Azure FedRAMP cloud environment. The FNCS FMS establishes and maintains its Azure subscriptions within the established United States Department of Agriculture (USDA) Digital Infrastructure Services Center (DISC) Azure tenant that defines the basic boundary of the system.

The FNCS FMSATO boundary is comprised of multiple sub-applications and system components. Those components which may process or store PII are:

- **Financial Management Application Toolset (FMAT)** is a financial management support solution that includes web-based custom-designed applications residing on the FNCS intranet. It is comprised of the following applications:
  - **Automated Entity Resolution and Optimization System (AEROS):** A custom solution providing the repository and mechanism for users to identify and match incoming collections to the appropriate customer and accounts receivable (AR) document. It provides a user interface for AR processors to view AR and collection-related data gathered from various systems, confirm data matches made by the system, and track and report on the status of collections throughout their lifecycle.
  - **Budget User Desktop Solution (BUDS):** An internal web-interface module that provides a process-driven SF-132 budget execution tool. BUDS enables end users to post SF-132 accounting events to the sub-allotment level and presents data in a user-friendly graphical interface.
  - **Grant Award Document and Letter of Credit (GAD/LOC) Amendments Process (GLAP):** Provides FNCS grantees with an Adobe Portable Document Format (PDF) version of their GAD/LOC amendments. The reports have been electronically signed and dated by an authorized FNCS employee in the Financial Management Modernization Initiative (FMMI).
  - The **FMAT Interface Module** supports the exchange of data between BUDS, IDEA, AEROS, GLAP, and the FMMI.
  - **Reporting** functionality to generate business reports for batch and user report requests is provided using SAP Business Objects.
  - The **UiPath Infrastructure:** Used to create process automation jobs as well automated test scripts for system validation and regression testing.
  - **FMAT-SQL PaaS:** Enabled the transfer of AEROS, BUDS and FMAT data from an on-premises SQL database server the MS Azure SQL PaaS environment.
- **Grants Information Management System (GIMS)** is a document management product that facilitates the management of all types and formats of content. It provides a secure, central repository for organizing and sharing content in an enterprise-wide fashion.

- **Food Programs Reporting System (FPRS)** is the primary FNCS tool for collecting, storing, tracking, and analyzing the Supplemental Nutrition Assistance Program (SNAP) and Special Nutrition information. FPRS is a browser-based application used by FNCS grantees to log in and submit regular required reports. It displays both financial and participation data related to the grants awarded.
- **National Data Bank (NDB)** supports the administration of all FNCS programs and is the official source of public information about FNCS. The system provides a single, consistent, official database to support analysis and public release of the mission area's program, financial, and audit information.

FM-GSS components that do not store, process, or transmit PII data are not described or included in this PIA.

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?

FNCS's legal authority for the collection of personally identifiable information (PII) is defined in 7 U.S.C. 2011-2031, Section 9 of the Food and Nutrition Act of 2008, as amended, (7 U.S.C. 2018). This provides the legal authority that permits the collection, use, maintenance, and sharing of PII, either generally or in support of a specific program or information system need.

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

CSAM: ATO Date/Expires: 11/28/2026

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

FNS-10, Food and Nutrition Service

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

No

Section 2.0 Characterization of the Information

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

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

The information that is used, disseminated, or maintained in FNCS FMS is related FNCS financial management processes.

- **FMAT:** The information that is used, disseminated, or maintained in **FMAT-AEROS** is related to vendors maintained in the Financial Management Modernization Initiative (FMMI) system including the vendor's name, business name, address, phone number, email IDs, STARS case number, check images along with signatures, bank account numbers and bank routing numbers from Treasury's Collection Information Repository (CIR) and Electronic Check Processing (ECP).
- **FMAT BUDS:** The information that is used, disseminated, or maintained in FMAT BUDS is related to payroll details in the Financial Management Modernization Initiative (FMMI) system. This information may include employee name, and pay and benefits data.
- **GIMS:** The information that is used, disseminated, or maintained in GIMS is related to FNCS discretionary grant programs. This may include the FNCS Request for Application (RFA), as well as data received via the Grants.gov application form download, such as the SF-424, SF-424A, SF-LLL, and Farm to School coversheet, as well as additional documents provided by grant applicants. In addition, approved GIMS users enter information needed to maintain official grant files, such as the applicant's employment history, key personnel salary data, or key personnel legal name, employer identification number (EIN), handwritten signatures, Grants.gov user ID, and address, as well as details related to grant pre-award, award and post-award.
- **FPRS:** Stores names, addresses, email addresses and phone numbers of users, in support of collecting, storing, tracking, and analyzing SNAP and Special Nutrition information.
- **NDB:** Stores SNAP and Special Nutrition information, along with names and email addresses of users.

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

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

Identifying Numbers			
☐	Social Security number	☐	Truncated or Partial Social Security number
☐	Driver's License Number	☐	License Plate Number
☐	Registration Number	☐	File/Case ID Number
☐	Student ID Number	☐	Federal Student Aid Number
☐	Passport number	☐	Alien Registration Number
☐	DOD ID Number	☐	DOD Benefits Number
☐	Employee Identification Number	☐	Professional License Number
☒	Taxpayer Identification Number	☐	Business Taxpayer Identification Number (sole proprietor)
☐	Credit/Debit Card Number	☐	Business Credit Card Number (sole proprietor)

Identifying Numbers

☐	Vehicle Identification Number	☐	Business Vehicle Identification Number (sole proprietor)
☒	Personal Bank Account Number	☐	Business Bank Account Number (sole proprietor)
☐	Personal Device Identifiers or Serial Numbers	☐	Business device identifiers or serial numbers (sole proprietor)
☐	Personal Mobile Number	☐	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number		

Biographical Information

☒	Name (including nicknames)	☐	Gender	☐	Business Mailing Address (sole proprietor)
☐	Date of Birth (MM/DD/YY)	☐	Ethnicity	☐	Business Phone or Fax Number (sole proprietor)
☐	Country of Birth	☐	City or County of Birth	☐	Group/Organization Membership
☐	Citizenship	☐	Immigration Status	☐	Religion/Religious Preference
☒	Home Address	☒	Zip Code	☒	Home Phone or Fax Number
☐	Spouse Information	☐		☐	Children Information
☐	Marital Status	☐	Military Service Information	☐	Mother's Maiden Name
☐	Race	☐	Nationality	☐	Global Positioning System (GPS)/Location Data
☒	Personal e-mail address	☒	Business e-mail address	☐	Personal Financial Information (including loan information)
☐	Employment Information	☐	Alias (username/screenname)	☐	Business Financial Information (including loan information)
☐	Education Information	☐	Resume or curriculum vitae	☐	Professional/personal references

Biometrics/Distinguishing Features/Characteristics

☐	Fingerprints	☐	Palm prints	☐	Vascular scans
☐	Retina/Iris Scans	☐	Dental Profile	☐	Scars, marks, tattoos
☐	Hair Color	☐	Eye Color	☐	Height
☐	Video recording	☐	Photos	☐	Voice/ Audio Recording
☐	DNA Sample or Profile	☐	Signatures	☐	Weight

Medical/Emergency Information

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

Device Information

☐	Device settings or preferences (e.g., security level, sharing options, ringtones)	☐	Cell tower records (e.g., logs, user location, time, etc.)	☐	Network communications data

Specific Information/File Types

☐	Personnel Files	☐	Law Enforcement Information	☐	Credit History Information

Identifying Numbers					
□	Health Information	□	Academic/Professional Background Information	□	Civil/Criminal History Information/Police Record
□	Case files	□	Security Clearance/Background Check	□	Taxpayer Information/Tax Return Information

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

FNCS FMS data is sourced from the applications hosted in boundary and transferred to connecting systems that process the data and may also be entered by USDA FNCS employees who have been approved for FNCS FMS access. Additional data sources are specific to the FNCS FMS module, as described below:

The data sources for **FMAT** include vendor and payroll data from FMMI; collection extract from Treasury's Collections Information Repository (CIR) system; and check images from Treasury's Electronic Check Processing (ECP) system.

The data sources for **GIMS** include grant applications submitted to Grants.gov, as well as data entered by USDA FNCS employees who have been approved for GIMS access.

The data sources for **FPRS** include commodity information from Web Based Supply Chain Management (WBSCM); FNS – E 152 data is imported from Automated Information System (AIS); and credentials from the eAuthentication system. Program and forms information is updated/entered by State, agency, regional, and Indian Tribe users. Administrators add and maintain information related to agencies and program-form participation in agencies.

The data sources for **NDB** include agency, program, form and submission information from FPRS; and commodity information from WBSCM.

2.2.1. How is the information collected?

Certificate-based mutual authentication is used, along with Secure Shell 2 (SSH-2), to transmit encrypted files and metadata from external applications into FNCS FMS applications. FNCS FMS application users have the ability to manually enter information in the processing application to assist them in managing their data.

- **FMAT** receives daily downloads from FMMI and the Treasury CIR & ECP systems, which is then uploaded into an encrypted database and the PII data is masked.

- **GIMS** downloads applications and data for those applications that have a Grants.gov status of "Validated."

- **FPRS** interfaces with the eAuthentication system to authenticate the users and stores the user information in the FPRS database. eAuth sends the user HTTPS header variable to FPRS, and FPRS verifies that a connecting user's credentials are at eAuth Level 2 and grants access to the user.

Commodity information is downloaded from WBSCM and uploaded to FPRS through the Administrator tab. FNS – E152 XML file is generated in the AIS system and uploaded to FPRS via the Submission studio.

Program and Forms information is updated/entered by State, agency, regional and Indian Tribe users. Administrators add and maintain information related to agencies and program-form participation in agencies.

- **NDB** uses automated ETL jobs to pick up the FPRS backup, restore and perform the ETL process. Once a month commodity data is downloaded from WBSCM as an Excel file and extracted – transformed – loaded (ETL) to NDB database. Administrators add and maintain user information via the NDB Admin tab.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?
No

2.4. How will the information be checked for accuracy? How often will it be checked?
FNCS FMS downloads "validated" data from externally connected applications and checks for accuracy once received. Transmission integrity is provided by SSH-2. SSH-2 which uses cryptographically strong Message Authentication Code (MAC) algorithms to provide integrity and data origin assurance.

- **FMAT** receives payment collections data from Treasury and it uses FMMI to match the existing vendor information or create a new vendor in order to process the collection document. FMAT does not check or index data retrieved from FMMI or Treasury. However, data checks ensure the data retrieved is the same data stored in the FMAT database. Transmission integrity is provided by SSH-2. SSH-2 uses cryptographically strong Message Authentication Code (MAC) algorithms to provide integrity and data origin assurance.

- **GIMS** downloads applications and data for those applications that have a Grants.gov status of "Validated." GIMS does not check or index data retrieved from Grants.gov. However, GIMS data checks ensure the data retrieved is the same data stored in the GIMS database. Transmission integrity is provided by SSH-2. SSH-2 uses cryptographically strong Message Authentication Code (MAC) algorithms to provide integrity and data origin assurance.

- **FPRS** has validations in place to ensure submission data adheres to pre-determined rules based on Agency, Program and Form. FPRS interfaces with the eAuthentication system to authenticate the users and stores the user information in the FPRS database. eAuth sends the user HTTPS header variable to FPRS, and FPRS verifies that a connecting user's credentials are at eAuth Level 2 and grants access to the user.

- **NDB's** ETL process has checks in place to validate the data from FPRS. NDB administrators verify the accuracy of the financial, participation, and all other submission related data. Administrators manually correct inaccuracies via the application during emergencies, however, as a general practice, agencies are expected to revise and resubmit inaccurate submissions in FPRS.

2.5. Does the system/program use third-party websites?
No

2.5.1. What is the purpose of the use of third-party websites?
Not applicable.

2.5.1.1. What PII will be made available to the agency though the use of third-party websites?
Not applicable

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

Privacy Risk: The collection of recipient name, mailing address, and financial data. And the collection of employers identification number (EIN) and vendor financial data

Mitigation:

- **GIMS:** These items are mitigated wholly or in part by: Using logical access controls, physical access controls, and personnel security controls. PII data not used for grants processing will be deleted and will not be stored in the GIMS database. PII data used for grant processing will be encrypted before archiving, before transmission, and in primary storage (i.e., the archive server). A notification will be included in the display when displaying PII. Outside of the GIMS applications specifics all FM-GSS database data is encrypted in transit and at rest.

  The employer identification number (EIN) or the taxpayer identification number will not be used in the grant award process after downloading from Grants.gov. The GIMS database will be encrypted. The un-redacted version of the file will be stored in encrypted zip files.

- **FMAT:** The vendor financial data confidentiality risks are mitigated using logical access controls, physical access controls to FMAT, and personnel security controls. PII data used for collection processing will be encrypted before saving.

  The FMAT database is encrypted along with the files received from Treasury. The FMMI files are deleted after they are loaded on to the database. All PII data is being masked in the database and only users with PII privileges will be able to view it. None of the users will have access to modify any PII data.

The payroll data confidentiality risks are mitigated using logical access controls, physical access controls to FMAT, and personnel security controls. PII data used for collection processing will be encrypted before saving.

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?

Data being processed in FNCS FMS cloud-based application systems support various FNCS program business functions and processes. Supported business functions and processes include, but are not limited to, grant opportunity establishment, application reception and distribution, award funding and determination, award generation, official grant-file-documentation maintenance and activities which support the discretionary grants award process throughout the life of an award.

- The information in **FMAT** is collected specifically for recouping payments, delinquent debts or overpayments owed to FNCS for a federal benefit program.

- The data in **GIMS** is used to support the discretionary grants award process at FNCS. This includes information for establishing grant opportunities, receiving applications, distributing applications for review, making award and funding decisions, generating awards, maintaining official grant file documentation and activities throughout the life of an award. FNCS is required to maintain official grant files with this information, per OMB grants guidance.

- **FPRS** is the primary FNCS tool for collecting, storing, tracking, and analyzing the Supplemental Nutrition Assistance Program (SNAP) and Special Nutrition information. FPRS used by FNCS grantees to log in and submit regular required reports. It displays both financial and participation data related to the grants awarded. User information is maintained to grant the needed access to the FPRS system.

- **NDB** supports the administration of all FNCS programs and is the official source of public information about FNCS. The system provides a single, consistent, official database to support analysis and public release of Agency program, financial, and audit information. User information is stored to authenticate users to the NDB system.

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

Yes

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

Privacy Risk: Disclosure of personal information

Mitigation:

- **GIMS:** Logical access controls, physical security controls, and personnel security controls are used to limit access to GIMS PII data based on least privileging and a need-to-know. OpenText xECM for SAP permissions to access data and execute OpenText xECM functionality are assigned to user roles. In addition, the OT archive server and database will encrypt all data. Data will be encrypted before transmission from or downloading from the GIMS. Further, certificate-based Mutual Authentication is used to gain access to grants.gov, and the data transmission is encrypted using SSH-2.

- **FMAT:** Logical access controls, physical security controls, and personnel security controls are used to limit access to FMAT PII data based on least privileging and a need-to-know. In addition, the FMAT database will be encrypted, along with the files received from Treasury. The FMMI files are deleted after they are uploaded to the database. Further, all PII data is being masked in the database and only users with PII privileges will be able to view it. None of the users will have access to modify any PII data.

- **FPRS:** communicates with the eAuthentication system to validate/authenticate users. Role based access controls are in place to ensure user access.

- **NDB:** uses role-based access controls to ensure user access.

Section 4.0 Notice

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

4.1. How does the project/program/system provide notice to individuals prior to collection?
This question applies to FNCS FMSGIMS only. A Privacy Statement is provided in the Privacy Policy section of the Request for Applications (RFAs). Applicants responding to FNCS RFA via Grants.gov are required to complete the federal forms which may contain PII data. FNCS downloads this information into GIMS via the Grants.gov interface on the application deadline as published in the RFA on Grants.gov.

4.2. What options are available for individuals to consent, decline, or opt out of the project?
This question applies to FNCS FMSGIMS only. Applicants responding to an FNCS RFA via Grants.gov are required to complete the federal forms which may contain PII data. If an application does not include all appropriate information, as noted in the RFA, FNCS will consider the application to be non-responsive and will eliminate it from further evaluation.

Only applications successfully submitted through the grants.gov web portal by the grantee are uploaded into GIMS.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

This question applies to FNCS FMSGIMS only.

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

Mitigation:
The notice is provided in the RFA under the section "Safeguarding Personally Identifiable Information" as follows:

> ***Safeguarding Personally Identifiable Information***
> *Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (National Institute of Standards and Technology (NIST) SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable information, April 2010).*
>
> *Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (National Institute of Standards and Technology (NIST) SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable information, April 2010).*
>
> *Applicants submitting applications in response to this RFA must recognize that confidentiality of PII and other sensitive data is of paramount importance to the USDA Food and Nutrition Service. All federal and non-federal employees (e.g., contractors, affiliates, or partners) working for or on behalf of FNS are required to acknowledge understanding of their responsibilities and accountability for using and protecting FNS PII in accordance with the Privacy Act of 1974; Office of Management and Budget Memorandum M-06-15, Safeguarding Personally Identifiable Information; M-06-16, Protection of Sensitive Agency Information; M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information; and the NIST Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.*
>
> *By submitting an application in response to this RFA, applicants are assuring that all data exchanges conducted throughout the application submission and pre-award process (and during the performance of the grant, if awarded) will be conducted in a manner consistent with applicable Federal laws. By submitting a grant application, applicants agree to take all necessary steps to protect such confidentiality, including the following: (1) ensuring that PII and sensitive data developed, obtained or otherwise associated with UDSA FNS funded grants is securely transmitted. Transmission of applications through Grants.gov is secure;*

(2) ensuring that PII is not transmitted to unauthorized users, and that PII and other sensitive data is not submitted via email; and (3) Data transmitted via approved file sharing services (WatchDox, ShareFile, etc.), CDs, DVDs, thumb drives, etc., must be encrypted.

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?

- **GIMS:** GIMS information is retained and archived in primary storage for six (6) years after the closeout of the program and archived per FNCS archival policy.

- **FMAT:** FMAT information is retained and archived in primary storage for six (6) years after final payment or cancellation.

- **FPRS, NDB:** FPRS and NDB don't purge any data stored in the applications.

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.
Yes, GRS 1.1, Item 010 see GRS 1.2, Item 010.

5.3. PRIVACY IMPACT ANALYSIS: **Related to retention of information.**
Privacy Risk: Disclosure of personal information

Mitigation:

- **GIMS** and **FMAT:** Data is retained and archived in GIMS and FMAT for a period of six (6) years and is encrypted in backup storage and primary storage. Any risks associated with the length of time is mitigated via data encryption. Archived data is encrypted in accordance with the FNCS policies.

- **FPRS** and **NDB:** FPRS and NDB don't purge any data stored in the applications.

Section 6.0 Information Sharing

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

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

- **FMAT:** In FMAT the vendor information will be used to create a new vendor in the FMMI system.

- **GIMS:** GIMS does not share PII with any other USDA information system. However, data from GIMS may be shared with internal FNCS organizations for the purpose of making award decisions and/or announcing awards. It may also be shared with external parties at the discretion of the Grants Director. For example, the agency Administrator or a Congressman may wish to obtain a list of applicants or awardees for a particular program.

- **FPRS:** FPRS shares the submission data and names of users who reported submissions to NDB.

- **NDB:** NDB uses the submission information to generate KeyData reports used for budget estimation and planning. NDB shares submission data and names of users who reported submissions with AGC. AGC's uses the data to analyze grants and spending data.

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

Privacy Risk: Disclosure of personal information

Mitigation: Access to FNCS FMS applications is authorized by the application Account Managers, identified by the System Owner. Data will be shared with external audiences, per the System Owner's discretion and approval.

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?

- **GIMS:** GIMS award results related information can be shared with a number of external parties, including, but not limited to, non-profit organizations, state and local organizations, individuals, corporations, and entities outside the U.S.

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

Privacy Risk: Disclosure of personal information

Mitigation: PII data shared with external review panelists will be encrypted. External review panelists will be required to sign a conflict of interest and non-disclosure agreement on an annual basis. Additionally, external review panelists will be required to complete annual PII training. Any GIMS data listed in Section 5.3 will be reviewed and approved by the Grants Director prior to distribution.

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?

Procedures for Redress outlined in SORN USDA/FNS–10. Located at: https://www.govinfo.gov/content/pkg/FR-2000-03-31/pdf/00-8005.pdf

7.2. What are the procedures for correcting inaccurate or erroneous information?
This question does not apply to FNCS FMSFMAT.

- **FMAT:** FMAT is not the system of records as the vendor PII information is captured through either FMMI or Treasury systems. As such, any data corrections required by the individual will be addressed by the corresponding systems.

- **GIMS:** If an applicant submits inaccurate or erroneous information, as noted in the RFA, FNCS will not consider additions or revisions to applications after the application deadline in Grants.gov. The grants officer may contact the applicant to resolve data discrepancies prior to making a grants decision award.

- **FPRS:** FPRS has validations in place to ensure submission data adheres to pre-determined rules based on Agency, Program and Form. If errors or inaccuracies exist in the data, agencies have to revise their submissions.

- **NDB:** NDB's ETL process has checks in place to validate the data from FPRS. NDB administrators verify the accuracy of the financial, participation, and all other submission related data. Administrators manually correct inaccuracies via the application during emergencies, however, as a general practice, agencies are expected to revise and resubmit inaccurate submissions in FPRS.

7.3. How are individuals notified of the procedures for correcting their information?
This question does not apply to FNCS FMSFMAT.

Procedures for individuals to correct their information are outlined in SORN USDA/FNS–10. Located at: https://www.govinfo.gov/content/pkg/FR-2000-03-31/pdf/00-8005.pdf

7.4. If no formal redress is provided, what alternatives are available to the individual?
None

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Privacy Risk: 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.

Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.