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.

Privacy Impact Assessment

Privacy Impact Assessment for the USDA IT System/Project:
Infrastructure General Support System (FNS – IGSS)

Office of Information Technology

Food, Nutrition, and Consumer Services

Date PIA submitted for review:
11/7/2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Deea Coleman FNCS Privacy Officer	deea.coleman@usda.gov	unlisted
Information System Security Manager	John Rosselot, Jr. Chief, Risk Management Branch	John.Rosselotjr@usda.gov	571-563-5260
System/Program Managers	Charles Hendricks	chuck.hendricks@usda.gov	415-645-1907
SAS Viya, Project Manager	James Morrison	James.morrison@usda.gov	816-266-5251

Privacy Impact Assessment

Abstract

This document is a Privacy Impact Assessment (PIA) for the FNS Infrastructure Services General Support System (FNS I-GSS) application SAS Viya.

SAS Viya is hosted in a USDA DISC-managed Azure Government cloud solution, as a "spoke" in the FNS Hub and Spoke architecture.

Overview

SAS Viya is a cloud-based in-memory analytics engine that provides data visualization, reporting and analytics to businesses for actionable data insights. It brings together visual analytics, visual statistics and data science for enterprises to achieve end-to-end self-service analytics. Analytics such as highlighting deviations from the baseline, forecasting information based on historic data, and data-driven decision making by combining best practice business models and ingested data.

SAS Viya does not collect PII; it ingests data from FNS Anti-Fraud Locator using EBT Retailer Transaction (ALERT), FNS Store Tracking and Redemption System (STARS), and the Office of Retailer Operations and Compliance.

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 CFR § 246.12 as the specific legal authority that defines the collection of information.

1.2 Has Authorization and Accreditation (A&A) been completed for the system?
Yes. SAS Viya is authorized as part of the FNS I-GSS boundary. The ATO expiration date is 9/30/2025.

1.3. What Systems of Records Notice(s) (SORN(s)) apply to the information?
N/A

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

Privacy Impact Assessment

Section 2.0 Characterization of the Information

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

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

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

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

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

Biographical Information					
☒	Name (including nicknames)	☐	Sex	☒	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
☐	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 information in the system/program?

Information is provided by the Office of Retailer Operations and Compliance (ROC), FNS ALERT, and FNS STARS.

2.2.1. How is the information collected?

SAS Viya does not collect information. The STARS and ALERT systems send their respective data to SAS Viya for analytics. SAS Viya stores data that other systems (STARS, ALERT) send to it. SAS Viya is used to perform analytics on that data.

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?

Accuracy of the information is the responsibility of the party of origin: ROC, STARS or ALERT

2.5. Does the system/program use third-party websites?
Not applicable

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 Information.

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

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.

Mitigation: By implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

User 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 users are aware of its characterization.

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?

Information is provided by the ROC, STARS, and ALERT to utilize SAS Viyas data analytics engine for the creation of reports, data visualizations and analytical insights.

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.

No

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

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user 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.

Mitigation: By implementing some or all the following mitigation actions, mission areas may safeguard PII better and ensure responsible use in compliance with PA requirement:

Purpose Limitation: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

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 the 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?

N/A. SAS Viya does not collect data from individuals.

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

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Privacy Risk: N/A

Mitigation: N/A

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?

SAS Viya stores data that other systems (STARS, ALERT) send to it.

FNCS will retain records in accordance with FNS – 91 N1-462-09-12 (ALERT records), and FNS – 85 N1-462-09-9 (STARS records).

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.

See 5.1.

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

Privacy Risk: Privacy act risks associated with the retention of information 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.

Mitigation: Implementing the following mitigation actions, mission areas can ensure responsible retention of PII while complying with the PA.

Data Retention Policy: Use NARA data retention policies that outline how long different types of PII will be retained and the rationale for those timeframes.

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.

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.

Access Controls: Implement strict access controls to limit who can view and manage retained personal information, reducing the risk of unauthorized access.

Data Minimization: Collect and retain only the PII that is necessary for the intended purpose, minimizing the risk associated with holding excessive data.

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?

Data is received from STARS, ALERT and the ROC.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.
Privacy Risk: Privacy risks associated with internal sharing and disclosure include:

Unauthorized Access: Employees may access PII without proper clearance, leading to potential misuse.

Data Breaches: Internal systems can be vulnerable to breaches, compromising PII.

Insider Threats: Employees with malicious intent may exploit their access to PII for personal gain.

Data Misuse: PII can be misused for purposes other than intended, leading to privacy violations.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Access Controls: Implement role-based access controls to limit who can access PII based on their job responsibilities.

Encryption: Use encryption for data in transit and at rest to protect PII from unauthorized access.

Regular Training: Provide ongoing training for employees on data privacy policies, the importance of protecting PII, and how to handle it securely.

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?

N/A. SAS Viya does not share information outside of USDA

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

Privacy Risk:

N/A. SAS Viya does not share information outside of USDA

Mitigation: N/A. SAS Viya does not share information outside of USDA

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?

NA. Redress is provided by the original source: FNS STARS, FNS ALERT, and the ROC

Redress is provided by the original source: FNS STARS, FNS ALERT, and the ROC

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

NA. Redress is provided by the original source: FNS STARS, FNS ALERT, and the ROC

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

NA. Redress is provided by the original source: FNS STARS, FNS ALERT, and the ROC

7.4. If no formal redress is provided, what alternatives are available to the individual?
NA. Redress is provided by the original source: FNS STARS, FNS ALERT, and ROC **7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.**

Privacy Risk: N/A.

Mitigation: N/A

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?

- Only authorized and authenticated users have access to the system.