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:

FNS Salesforce | Store Visit Contract (SVC)

Food, Nutrition, and Consumer Service (FNCS)

Date PIA submitted for review:
5/15/2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	Deea Coleman	Deea.Coleman@usda.gov	unlisted
Information System Security Manager	John Rosselot Chief, Risk Management Branch	John.Rosselot@usda.gov	571-563-5260
Project Manager, SVC	Erin McBride	erin.mcbride@usda.gov	703-305-2709

Privacy Impact Assessment

Abstract

The Store Visit Contract (SVC) is built upon the Salesforce GovCloudPlus platform, which is FedRAMP authorized and is managed and operated by Manhattan Sales Group (MSG). SVC receives, processes, and delivers retailer data in support of the Supplemental Nutrition Assistance Program (SNAP); the retailers participate in the SNAP program and, as such, are subject to site visits to validate and verify operations. This PIA is required as there are certain personally identifiable information (PII) data elements included in the information collected from the participating retailer, and transmitted from SVC via the Retail File System (RFS) to Store Tracking and Reporting System (STARS).

Overview

Store Visit Contract (SVC) utilizes the Salesforce GovCloud Plus platform to service the SNAP Retailer Visit Contract. The Store Visit Contract (SVC) is built upon the Salesforce GovCloudPlus platform, which is FedRAMP authorized and is managed and operated by Manhattan Sales Group (MSG). SVC receives, processes, and delivers retailer data in support of the Supplemental Nutrition Assistance Program (SNAP); the retailers participate in the SNAP program and, as such, are subject to site visits to validate and verify operations.

The Food, Nutrition, and Consumer Service (FNCS) Office of Information Technology (OIT) Program Management Division (PMD) provides project management oversight of the SVC system. SNAP is the FNCS program (business unit) that uses the application.

SVC receives, processes, and delivers retailer data, including retailer personally identifiable information (PII), via the Retail File System (RFS) to Store Tracking and Reporting System (STARS). The data delivered is vital to allow SNAP to make informed decisions regarding retailer eligibility to accept SNAP benefits, continuous re-authorization of that eligibility, and take administrative actions as necessary. PII collected is limited to participating retailers and related business information: store/retail owner's name, business address, business email, vehicle identification numbers, and license plate numbers (to track food deliveries).

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 Systems of Records Notice (SORN) applies, if an Authorization To Operate (ATO) has been completed and if there is a Paperwork Reduction Act coverage.

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

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

7 U.S. Code Chapter 51, 2018, Sec. 9.10(a)(1)(D) states no retailer food store or wholesale food concern shall be approved to be authorized or reauthorized for participation in SNAP unless a store visit has been conducted.

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

Yes. SVC is authorized as part of the FNS Salesforce boundary. The most recent authorization was granted on 8/21/2023 and expires 8/26/2026.

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

Yes. SORN USDA/FNCS-12, 2021-21941.pdf (govinfo.gov). This SORN maintains records of activities conducted pursuant to FNCS' mission and responsibilities authorized by legislation. 7 CFR § 246.12 is the specific legal authority that defines the collection of information.

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?

Information about the retail establishment is collected by the SVC Reviewers. Non PII data elements include retail establishment's general characteristics, food and non-food inventory, and photographs of the store itself and its contents. PII data collected is the store owner's name, as well as delivery vehicle information (VIN and license plate number). The information is used for SNAP retailer application processing, re-authorization procedures, and enforcement actions. The information is maintained in the SVC system for a period of 18 months before it is permanently removed.

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

Privacy Impact Assessment

Identifying Numbers			
☐	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)	☐	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	☐	Sexual Orientation	☐	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

Identifying Numbers					
☐	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 the information in the system/program?

SVC uses information provided by the retailer, as well as by FNCS from the tangential retailer's SNAP participation application.

2.2.1. How is the information collected?

Information is provided during the SNAP application process.

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

Commercial information is provided by the retailer and FNCS during the SNAP application process. Some of the information collected, such as business address, is publicly available.

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

SVC utilizes a team of Quality Control personnel to compare store visit survey data against photographic support collected at the same time of the visit.

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?

Third-party websites are not used.

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

Third-party websites are not used.

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

Privacy Risk: The privacy risks associated with SVC are centered around the unauthorized disclosure of the PII hosted on the platform.

Mitigation: MSG utilizes Salesforce's Shield Platform Encryption to mitigate the threat to unauthorized disclosure of PII. With Shield Platform Encryption, the System Administrator can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports user accounts, cases, search, approval processes, and other key Salesforce features. Access to SVC is also tightly controlled through the use of eAuthentication and least role privileges.

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?

FNCS uses the retailer information to make informed decisions regarding retailer eligibility to join SNAP and accept benefits from the public. The information allows FNCS to ensure the authorized retailers can provide enough nutritious supplement to the local communities that rely on the support to feed families and to reduce food deserts. FNCS will use the data to continuously monitor and reauthorize retailers to continue participating in the program. The information also assists FNCS in taking decisive action when it comes to non-compliance of program regulations

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.

Tools used are Salesforce Reports, and Salesforce Dashboards. All of these tools can produce reports or graphics that can summarize the data. Data is used to continuously monitor and reauthorize retailers to continue participating in the program.

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

Privacy Risk: The privacy risks related to the use of information are centered around compromising information that is being stored.

Mitigation: 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 the information that is being stored. 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.

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?

When completing the FNS-674 form, contractors and partners will sign an acknowledgement of understanding the Privacy Act Statement is provided within the document.

Retailers applying or participating in SNAP are informed that store visits are required. Prior to beginning the store visit, retailers are given the option to consent to the unannounced visit. Providing consent allows the SVC Reviewer to collect retailer information.

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

Retailers are given the option to consent to the unannounced visit. Providing consent allows the SVC Reviewer to collect retailer information.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Privacy Risk: The privacy risks related to notice are focused on the collection of data from retailors with or without their consent.

Mitigation: Retailers are given the option to consent to the unannounced visit. Providing consent allows the SVC Reviewer to collect retailer information.

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 for a total of 18 months. SVC will retain retailer information for a period of one (1) year of being confirmed. After one (1) year, Salesforce will transfer the deliverables to an AWS S3 repository for cold storage. The data within AWS S3 can only be accessed and retrieved by authorized privileged users. After six (6) months, the retailer information is removed from AWS S3 permanently.

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: All record retention schedules are found in Section 5.1, the name of the records retention schedule is FNCS Electronic Information System Questionnaire for Records Management Scheduling.

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

Privacy Risk: The privacy related risk associated with data retention are primarily centered around the increase of exposure to data leaks that is inherit with storing more data than necessary.

Mitigation: The records schedule proposed to NARA represents ideal timelines for records retention and disposal. Maintenance and destruction timelines mitigate data protection risk and ensure currency of information.

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?

SVC transmit retailor information via Retail File System (RFS) to Store Tracking and Reporting System (STARS). This information includes retailer ownership details, retailer general characteristics, food and non-food inventory, retailer delivery vehicle information, and photographs of the store and its contents. The information shared enables FNCS to make informed decisions regarding retailer eligibility to accept SNAP benefits, continuous re-authorization, and take administrative actions.

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

Privacy Risk: The privacy risks are centered around the unauthorized disclosure of the PII hosted in the MSG Salesforce environment.

Mitigation: MSG utilizes Salesforce's Shield Platform Encryption to mitigate the threat to unauthorized disclosure of PII. With Shield Platform Encryption, the System Administrator can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports user accounts, cases, search, approval processes, and other key features. Access to SVC is also tightly controlled through the use of eAuthentication and least role privileges.

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?

FNCS transmits retailer information via secure web-services that require authorized user credentials to access Salesforce and provide retailer information. Salesforce, in return, will use secure web-services using authorized user credentials to transmit the store visit deliverables. Users requesting access to these user credentials and web-service setup must go through written request and background clearance. A separate login and e-authentication is required to access RFS and STARS.

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

Privacy Risk: The privacy risks are centered around the unauthorized disclosure of the PII hosted on the platform.

Mitigation: MSG utilizes Salesforce's Shield Platform Encryption to mitigate the threat to unauthorized disclosure of PII. With Shield Platform Encryption, the System Administrator can encrypt a variety of widely used standard fields, along with some custom fields and many kinds of files. Shield Platform Encryption also supports user accounts, cases, search, approval processes, and other key features. Access to SVC is also tightly controlled through the use of eAuthentication and least role privileges.

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?

Retailers do not have access to their information. Retailers may contact FNCS directly via the Retailer Service Center (RSC) if they would like to request access to their information.

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

SVC Reviewers allow retailer personnel to provide retailer information, including retailer PII. The information is collected and securely transmitted from SVC via RFS to STARS for FNCS review. The retailer may opt to make a correction at the time of the visit where the correct information will be documented. Alternatively, the retailer may contact the retailer call center for further guidance.

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

If the information collected is incorrect, the individual has an opportunity to provide the correct information to the SVC Reviewer at the time of the visit. In addition, they may also contact the RSC to address any issues.

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

If formal redress is not possible after contacting FNCS or the RSC in accordance with established procedures, individuals are directed to utilize other legal measures to correct erroneous information, including but not limited to, filing civil and/or criminal complaints.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Privacy Risk: The privacy risks are centered around the unauthorized disclosure of the PII hosted on the platform.

Mitigation: Individuals concerned that their PII data may have been compromised may contact the USDA office designated within the System of Records notice posted in the Federal Register.

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?

SVC built upon the Salesforce GovCloud platform, utilizes a robust collection of technical safeguards to ensure the integrity of the platform. SVC is hosted in a secure server environment that uses a firewall to prevent interference or access from outside intruders. When accessing SVC, Secure Socket Layer (SSL) technology protects the user's information by using both server authentication and data encryption. SVC administrators will have a suite of security tools that can be used to increase the security of the system. From a physical security standpoint, the servers that host SVC are stored in a privately owned data center with strict physical access control procedures in place to prevent unauthorized access.

Access to systems inside of the Salesforce Government Cloud storing U.S. government, U.S. government contractors, and customer data that potentially permit access to customer data are restricted to Qualified U.S. Citizens. Qualified U.S. Citizens are individuals who are United States citizens, are physically located within the United States when accessing the Salesforce Government Cloud systems and have completed a background check as a condition of their employment with Salesforce.

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

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 the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know to the information for the performance of their official duties and who have appropriate clearances or permissions.

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

Information sharing requirements are reviewed and approved on a yearly basis according to our annual assessment and review schedule.

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