Privacy Impact Assessment
Template

Policy, E-Government and Fair Information Practices

- Version: 1.5
- Date: July 16, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA
United States Department
of Agriculture

Privacy Impact Assessment for the

Store Tracking And Redemption System (STARS)

July 2020

Contact Point

Vance Parker
System Owner/FNS/OIT/PMD
703-305-2777

Reviewing Official

Miguel Marling
Privacy Officer
United States Department of Agriculture
703-305-1627

Abstract

A PIA is being performed on the Store Tracking and Redemption System (STARS). STARS stores information on retailers that participate in the Supplemental Nutrition Assistance Program (SNAP). This system is used by various federal and state users to track, monitor, and assess retailers. A PIA is being conducted due to the content within STARS and the controls protecting that data.

Overview

The Retailer participation in the SNAP program is administered through a headquarters organization, primarily the Retailer Operations and Compliance (ROC) and the Retailer Policy and Management Division (RPMD). The ROC is responsible for the overall management and direction of activities related to the operational components of retailer management. These include compliance functions – i.e. identifying, investigating, and taking administrative action on suspected program violators, as well as the authorization/reauthorization function. RPMD is responsible for national retailer management regulation, policy and guidance development, EBT issuance, systems oversight and development, quality assurance, training, budget management, contracting, and the administrative review function. A team of out-stationed compliance investigators report to headquarters through regional compliance area offices. These organizations are responsible for managing the benefit redemption functions of the SNAP. Cooperating state and local agencies with FNS oversight perform benefit issuance functions.

FNS is responsible for approving retail firms and community meal services and programs in order for them to be able to exchange SNAP benefits for food. The Agency accepts and reviews store and meal service applications for approval. To do this, FNS operates a Store Tracking and Redemption System (STARS) which maintains store identification, location, ownership and monitoring data. STARS also maintains investigative and sanction information as well as authorization and redemption information. Retailers may not legally accept SNAP benefits without being authorized to do so by FNS.

There are over 700 active STARS IDs issued for direct access to add, delete, and update data and to inquire the status of store redemptions, authorizations and investigations for the over 250,000 grocery stores and specialized meal services authorized to accept SNAP benefits. These users include, but are not limited to, the officials responsible for SNAP administration and investigation in FNS, the USDA Office of the Inspector General (OIG), SNAP State agencies as well as the State agencies administering the Women, Infants, and Children (WIC) Program.

The general data type to be used in this system could be classified as public or, at most sensitive, "business sensitive" (when covering sales figures and such). The information in the STARS system includes SSNs and home addresses for most of the store owners participating or applying to participate in the SNAP. The vast majority of the information in the system is not "private" (covered under the Privacy Act). Nor does the system require this data in all cases. Any potentially sensitive information such as SSN is stored encrypted in the database. All data, regardless of sensitivity, is transmitted via HTTPS while in motion between the client and the servers.

Section 9 of the Food Stamp Act of 1977, as amended, (7 U.S.C. 2018) and section 1735 of the Food, Agriculture, Conservation, and Trade Act of 1990 (Pub. L. 101—624, 104 Stat. 3359) authorizes collection of SSN/TIN information of program applicants.

Section 1.0 Characterization of the Information

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

1.1 What information is collected, used, disseminated, or maintained in the system?

STARS collects the name, address, applicant's social security number, birth date and store owners Employer ID Numbers. In addition, the system collects the name and email address of the system users. Financial Information such as the Sales Data – annual sales information from retailers per food category is collected from new applicants and those requesting re-authorization to ensure compliance with regulations. Sales Data are not requested every year once authorized.

1.2 What are the sources of the information in the system?

Store owners wanting to participate in the program offer their own information. Also, Electronic Benefit Transfer (EBT) processors provide redemption information for each store in the program

1.3 Why is the information being collected, used, disseminated, or maintained?

The store owner information is used to determine if the owner has a negative history with the SNAP program and can be used as a denial reason for future applications. For the store redemption information from the EBT processors, that information is used to determine if a store is still active within the SNAP program.

For system user information, their name and e-Authentication ID are used to track their actions within the system and their email address is used to send technical tips, release notes, notifications of system outages and planned maintenance to them. In some cases the user name is utilized on letters sent on their behalf to store owners.

1.4 How is the information collected?

Store owners, when filling out applications to participate in the program, offer their information through a website or in a paper form.

On a weekly basis, Electronic Benefit Transfer (EBT) processors provide redemption information for each store in the program.

1.5 How will the information be checked for accuracy?

Store information is collected and reviewed. As part of the application process, the application data in some cases is verified with a visit to the store. Store owners (program applicants) are the source for the more sensitive privacy data.

System user information is taken directly from the USDA e-Authentication system and is assumed accurate.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Food and Nutrition Act 2008

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

All PII data is encrypted at rest and in transit. Access to the data is tightly controlled through the use of e-Authentication and least role privileges.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

Owner data collected is used to provide history information of that store owner within the SNAP program. The system only keeps information on store owners and their relationship to stores within the Supplemental Nutrition Assistance Program (SNAP). Information contains the name, Social Security Number, Birth date, address, relationship to the store, and if any violations are related to that individual. All of this is identified in the System of Record and is outlined in writing in the FNS-252 form filled out by the store owner.

2.2 What types of tools are used to analyze data and what type of data may be produced?

Data is stored in Microsoft SQL server (PII encrypted) and is accessed by the application only. No other commercial tools are used.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Not Applicable. STARS does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

All PII data is encrypted at rest and in transit. Access to the data is tightly controlled through the use of e-Authentication and least role privileges.

Section 3.0 Retention

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

3.1 How long is information retained?

Destroy 6 years after termination of system and successful migration of data or termination of system.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. N1-462-09-9

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Keeping Privacy information does pose a risk. All PII data is encrypted at rest and in transit.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

These users include, but are not limited to, the officials responsible for SNAP administration and investigation in FNS, the USDA Office of the Inspector General (OIG), SNAP State agencies as well as the State agencies administering the Women, Infants, and Children (WIC) Program.

4.2 How is the information transmitted or disclosed?

All information collected is provided by the user (internal organization officials listed in 4.1) logging into the system using their approved credentials.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Any privacy is mitigated by ensuring that the correct people have proper access to the system and roles and permissions are assigned accordingly.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The state SNAP and WIC agencies use this information. State Agencies use this information to investigate client and/or retailer fraud, to simplify the WIC retailer application process, and to assist in managing their respective areas of responsibility.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it

covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Yes. FNS-9 https://www.federalregister.gov/articles/2010/12/27/2010-32457/privacy- act-revision-of-privacy-act-systems-of-records#p-30

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

Each State Agency is required to have a security officer to manage requests and provide oversight relative to State Agency system access. FNS regional and HQ security must also approve access to the system.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Each State Agency is required to have a security officer to manage requests and provide oversight relative to State Agency system access. FNS regional and HQ security must also approve access to the system. The system is designed to be used across all sites with the same role-based access controls and safeguards at all sites.

Section 6.0 Notice

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

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

Yes. FNS-9 https://www.federalregister.gov/articles/2010/12/27/2010-32457/privacy-act-revision-of-privacy-act-systems-of-records#p-30

6.2 Was notice provided to the individual prior to collection of information?

Yes

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Store owners, when filling out applications to participate in the program, offer their information. Later, store information is collected and reviewed. As part of the application process the application data in some cases is verified with a visit to the store. Store owners (program applicants) are the source for the more sensitive privacy data. If they decline, their application cannot be processed.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Store owners, when filling out applications to participate in the program, offer their information. Later, store information is collected and reviewed. As part of the application process the application data in some cases is verified with a visit to the store. Store owners (program applicants) are the source for the more sensitive privacy data. If they decline, their application cannot be processed.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

See System of Record Notice. Store Owners supply their information on a form requesting that their store be allowed to accept SNAP benefits. Further they must also supply proof that the information that they submit is accurate. If they refuse to supply that information their application cannot be processed and their store will not be allowed to accept SNAP benefits.

Section 7.0 Access, Redress and Correction

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

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

They can call the STARS help desk or contact their local field or regional office.

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

They can call the STARS help desk or contact their local field or regional office.

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

They can call the STARS help desk or contact their local field or regional office.

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

They can call the STARS help desk or contact their local field or regional office.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

The system does track store owners and their relationship to stores but all investigations and actions are done against stores and not individual store owners. This insures that there is equitable treatment of store owners (Customers).

Section 8.0 Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

FNS employees who have responsibility for stores in the SNAP program will have access to customer information. State SNAP program registered users will have access only to the customer name and store redemption history. They will not have access to other privacy information. Developers and Quality Assurance personnel do not have access to social security information or to the live system. System administrators have access to all information.

8.2 Will Department contractors have access to the system?

Contractors will have access to the system as needed.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Privacy training is part of the annual security awareness training that all employees and contractors must complete prior to being granted access to any FNS system.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

The current ATO is dated May 18, 2018

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

All PII data is encrypted at rest and in transit. User access is done through the use of e- Authentication and roles of least privileges. All user activity is logged. Users can not create ad-hoc reports and access to privacy data is limited.

8.6 <u>Privacy Impact Analysis</u>: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

All PII data is encrypted at rest and in transit. User access is done through the use of e- Authentication and roles of least privileges. All user activity is logged. Users can not create ad-hoc reports and access to privacy data is limited.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

This application is written in AngularJS, Bootstrap, HTML5, JAVA and uses WildFly application server. The database is Microsoft SQL Server.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23

"Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Not Applicable. No use of 3rd party website and/or applications.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

Not Applicable. No use of 3rd party website and/or applications.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

Not Applicable. No use of 3rd party website and/or applications.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

Not Applicable. No use of 3rd party website and/or applications.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

Not Applicable. No use of 3rd party website and/or applications.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not Applicable. No use of 3rd party website and/or applications.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Not Applicable. No use of 3rd party website and/or applications.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not Applicable. No use of 3rd party website and/or applications.

10.10 Does the system use web measurement and customization technology?

No

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

Not Applicable.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not Applicable. No use of 3rd party website and/or applications.

Agency Responsible Officials

Digitally signed by CATRINA LEE
'Date: 2020.08.11 13:11:00 -05'00

Catrina L Lee

Catrina L Lee
IT Project Manager
Operations and Maintenance Branch
Portfolio Management Division
Food and Nutrition Service
United States Department of Agriculture

Date

VANCE PARKER

Digitally signed by VANCE PARKER
Date: 2020.08.11 14:28:46 -04'00'

Vance Parker
System Owner
Director, Portfolio Management Division
Food and Nutrition Service
United States Department of Agriculture

Date

Agency Approval Signature

JOSEPH BINNS

Digitally signed by JOSEPH BINNS
Date: 2020.08.12 10:34:16 -04'00'

Joseph Binns
ISSPM/CISO
Food and Nutrition Service
United States Department of Agriculture

Date