Privacy Impact Assessment
Food Delivery Portal (FDP)

Food Delivery Portal (FDP)

- Version: 1.0
- Date: November 20, 2020
- Prepared for: USDA OCIO-Policy and Directives - Privacy Office

United States Department of Agriculture

Privacy Impact Assessment for the

Food and Nutrition Service, Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) Food Delivery Portal (FDP)

November 20, 2020

Contact Point
Kelly Jackson – Information Owner
Food and Nutrition Service
United States Department of Agriculture
703-305-2677

Reviewing Official
Miguel Marling – Privacy Officer
Food and Nutrition Service
United States Department of Agriculture
(703) 305-1627

Abstract

Food Delivery Portal (FDP) will replace The Integrity Profile (TIP) as the system used to house State agency vendor management data for the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC), which is operated by the Department of Agriculture's Food and Nutrition Service (FNS). The data housed in FDP will be critical to providing effective federal oversight of the WIC Program, because the data informs FNS on State agency performance regarding vendor training, compliance, monitoring, and sanctions. A Privacy Impact Assessment (PIA) is being conducted because FDP contains personally identifiable information (PII), specifically full names, business tax identification numbers, and assigned agency numbers.

Overview

Food Delivery Portal (FDP) is owned and operated by the Department of Agriculture's Food and Nutrition Service (FNS). FDP will host vendor management data submitted by State agencies for the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) and will be critical to providing effective federal oversight of the WIC Program. FDP will contain information on State agency performance regarding vendor training, visits, investigations, violations, sanctions, compliance, monitoring, and redemptions as well as vendor information such as store name, store address, tax identification number, and assigned agency number. An example of a typical transaction within FDP is a State agency uploading vendor information into the platform, or FNS users searching for vendor information by the tax identification number. FNS routinely shares information that is housed within FDP. These routine uses include sharing information for the purposes of audits and oversight; for Congressional inquiries; for disclosure to contractors as outlined under the Privacy Act of 1974, as amended, pursuant to 5 USC § 552a(m); for disclosure to the National Archives and Records Administration; for disclosure to State agencies; and as mandated by law for information security breaches. FDP utilizes several modules, which include USDA's eAuthentication system, MuleSoft, TIP, and UDSA's Store Tracking and Redemption System (STARS). eAuthentication is the system used by USDA agencies that enables individual customers and employees to obtain a single account that will allow them to access USDA Web applications and services via the Internet. MuleSoft is an integration platform that will allow FNS to access, transform and serve up data from 3rd party external systems and internal FNS systems (e.g., STARS, TIP) in a secure, scalable manner at a lower level of effort. TIP is the legacy application database that was previously used to house State agency vendor management data for the WIC Program. STARS is the USDA database that stores information on retailers that participate in the Supplemental Nutrition Assistance Program (SNAP). 7 CFR § 246.12 is the specific legal authority that FNS uses to collect the information housed in FDP.

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?

FDP collects information on WIC vendor management activities and vendor data. State agency policy data and Food Delivery Entity (FDE) vendors are the subjects of records in FDP. Specific information maintained on those subjects includes policy data, state agency users, annual vendor data, training, redemptions, investigations, violations, compliance buys, sanctions, hours of operation, store owners and account history. These records are maintained on each State agency and FDE once they decide to participate in the WIC Program and after they leave the WIC Program.

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

The vendor management data that will be stored within FDP will be submitted by WIC State agencies. Data was also migrated from The Integrity Profile (TIP) during development of FDP.

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

The information is collected so that FNS can provide effective federal oversite over the WIC Program. The information will be used to inform FNS on State agency performance regarding vendor training, compliance, monitoring, and sanctions.

1.4 How is the information collected?

There are several ways that the vendor management data can be input into FDP. State agency users can either manually input data into the system or can upload data by using CSV and XML files. The WIC Program also has a data sharing agreement with the SNAP, which imports data between FDP and the Store Tracking and Reporting System (STARS) systems.

1.5 How will the information be checked for accuracy?

Vendor management data that is submitted into FDP will be checked for accuracy through validation checks to ensure that the data is accurate before it is saved in the system. FNS will also review reports generated by FDP to ensure data accuracy.

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

7 CFR § 246.12 is the specific legal authority that defines the collection of information. New System of Records (SOR) Notice (SORN) entitled USDA/FNS-12, Food Delivery Portal (FDP), which will replace The Integrity Profile (TIP) as the system used to house State agency vendor management data for the Special Supplemental Nutrition Program (SNAP) for Women, Infants, and Children (WIC), is in routing for approval to/thru the Departmental Privacy Office under the Office of the Chief Information Officer using the Executive Correspondence Management system. This SOR maintains records of activities conducted pursuant to FNS' mission and responsibilities authorized by legislation.

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

The privacy risks associated with FDP are centered around the unauthorized disclosure of the personally identifiable information (PII) hosted on the platform. FDP utilizes 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 FDP features. Access to FDP is also tightly controlled through the use of eAuthentication 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.

FNS uses the information on vendor management activities and vendor data to provide effective federal oversight of the WIC Program. The data analytics options within FDP will allow FNS to analyze nationwide trends in vendor and contractor data while also providing assurances to Congress, the Office of Inspector General, senior program managers and the general public that every reasonable effort is being made to prevent, detect and eliminate fraud, waste, and abuse. FDP will support FNS in formulating program policies and regulations, generating an annual report to assess State agency progress in assessing the level of activity that is being completed to ensure program integrity, and analyzing trends over a 5-year period.

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

FDP will support several tools to analyze data, including Salesforce Reports, Salesforce Dashboards, and Tableau. All of these tools can produce reports or graphics that can summarize the data.

A Salesforce Report is a list of records that meet a specific set of criteria defined by the user. It's displayed in Salesforce in rows and columns, and can be filtered, grouped, or displayed in a graphical chart. Every report is stored in a folder. Folders can be public, hidden, or shared, and can be set to read-only or read/write. Administrators control who has access to the contents of the folder based on roles, permissions, public groups, and license types.

Salesforce Dashboards offer a visual display of key metrics and trends for records. The relationship between a dashboard component and report is 1:1; for each dashboard component, there is a single underlying report. However, the same report can be used in multiple dashboard components on a single dashboard (e.g., use the same report in both a bar chart and pie chart). Multiple dashboard components can be shown together on a single dashboard page layout, creating a powerful visual display and a way to consume multiple reports that often have a common theme. Like reports, dashboards are stored in folders, which control access. If a user has access to a folder then the user can also view dashboards within the folder. However, to view the dashboard components, the user would also need access to the underlying reports as well.

Tableau is a visual analytics platform that enables the user to explore, analyze, manage, and share data.

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

FDP utilizes commercial Geographic Information System (GIS) mapping to map the location of vendor stores.

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.

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.

FDP utilizes a robust collection of technical safeguards to ensure the integrity of the platform. FDP is hosted in a secure server environment that uses a firewall to prevent interference or access from outside intruders. When accessing FDP, Secure Socket Layer (SSL) technology protects the user's information by using both server authentication and data encryption. FDP 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 FDP are stored in a privately owned data center with strict physical access control procedures in place to prevent unauthorized access.

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?

FDP does not have currently have a records schedule that is approved by the National Archives and Records Administration (NARA). The proposed schedule dictates that the different information sets will be retained for different periods of time, as described below. The records within FDP will be kept indefinitely until NARA has approved a records schedule for FDP.

FDP's Database/Master file will be retained on a temporary basis and will be destroyed either 10 years after the termination of the system and the successful migration of the data or 10 years after the termination of the system.

The Electronic Food Delivery Portal Data Entry Form, which represents an Input to FDP, will be retained in accordance with GRS 5.2, Item 020 on a temporary basis and destroyed upon verification of the successful creation of the final document or file, or when no longer needed for business use, whichever is later.

Outputs and Reports generated by FDP, which will be retained in accordance with GRS 5.2, Item 020, can be in any of the following formats: electronic, metadata, reference data, or paper. Outputs and Reports will be kept on a temporary basis and destroyed upon verification of the successful creation of the final document or file, or when no longer needed for business use, whichever is later.

System Documentation for FDP will be retained in accordance with GRS 3.1, Item 051. System Documentation for FDP includes data system specifications, file specifications, codebooks, record layouts, user guides, output specifications, and final reports (regardless of medium) relating to a master file, database or other electronic records. System Documentation will be retained on a temporary basis and destroyed 5 years after the project/activity/transaction is completed or superseded, or when the associated system is terminated, or when the associated data is migrated to a successor system.

The information in FDP will be retained on the abovementioned schedule to allow FNS to analyze nationwide trends in vendor and contractor data while also providing assurances to Congress, the Office of Inspector General, senior program managers and the general public that every reasonable effort is being made to prevent, detect and eliminate fraud, waste, and abuse. FDP will support FNS in formulating program policies and regulations, generating an annual report to assess State agency progress in assessing the level of activity that is being completed to ensure program integrity, and analyzing trends over a 5-year period.

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

The proposed retention period has not yet been approved by NARA.

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

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 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?

Employees and contractors from the Department's FNS Program Integrity and Monitoring Branch (PIMB) are responsible for conducting federal oversight of the WIC Program and are the primary users of the information housed within FDP. SNAP will be able to access a portion of the data housed within FDP, in order to facilitate review of and reporting on food providers that exist in both Programs. Additional Programs operated by the Department, within FNS, may also receive a designated sub-set of data in the future.

4.2 How is the information transmitted or disclosed?

Users can access FDP by using their eAuthentication login 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.

The privacy risks associated with FDP are centered around the unauthorized disclosure of the personally identifiable information (PII) hosted on the platform. FDP utilizes 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 FDP features. Access to FDP is also tightly controlled through the use of eAuthentication and least role privileges.

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?

Consistent with USDA's information sharing mission, information stored in FDP may be shared with other USDA components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after USDA determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in FDP's System of Records Notice, which are also described below.

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside USDA as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

(1) To the Department of Justice (DOJ), including Offices of the United States Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

(2) To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

(3) To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

(4) To an appropriate federal, state, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

(5) Disclosure to contractors under section (m): To agency contractors, grantees, experts, consultants or volunteers who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 USC § 552a(m).

(6) Disclosure to NARA: Records from this SOR may be disclosed to the National Archives and Records Administration (NARA) or to the General Services Administration for records management inspections conducted under 44 USC § 2904 and § 2906.

(7) Disclosure to State agencies: For State agencies to conduct any activities that are necessary to remain in compliance with the WIC Program requirements.

(8) Information security breaches: To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that the security or confidentiality of information in

the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

(9) To another Federal agency or Federal entity, when USDA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

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.

The sharing of PII is compatible with the original collection and will be done in accordance with the routine uses outlined in Section 5.1

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

There is currently no expectation that sensitive data from FDP will be shared outside of the USDA except as in 5.1 and 5.2 above. If a requirement to share such data were to arise in the future, the data would be protected in accordance with Federal requirements, to include the use of approved encryption mechanisms.

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

The privacy risks associated with FDP are centered around the unauthorized disclosure of the personally identifiable information (PII) hosted on the platform. FDP utilizes 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 FDP features. Access to FDP is also tightly controlled through the use of eAuthentication and least role privileges.

However, FNS does not share PII housed in FDP with any source outside of USDA, so there are no privacy risks to mitigate.

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. New SORN USDA/FNS-12, Food Delivery Portal (FDP), is in routing for approval to/thru the Departmental Privacy Office under the Office of the Chief Information Officer using the Executive Correspondence Management system. This SOR maintains records of activities conducted pursuant to FNS' mission and responsibilities authorized by legislation. 7 CFR § 246.12 is the specific legal authority that defines the collection of information. A URL is yet to be established.

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

State Agencies and vendors who choose to participate in the WIC Program are required to submit specific information to FNS. State Agencies and vendors are notified of the program and information collection authorities and prior to participating including Privacy Act Statements when applicable.

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

Vendors and State agencies who choose to participate in the WIC Program do not have the opportunity and/or right to decline to provide required information.

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

Vendors and State agencies who choose to participate in the WIC Program do not have the right to consent to particular uses of the information.

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.

Notice is provided to the Vendors and State Agencies who choose to participate in the WIC Program during their initial onboarding process. There is no risk with the vendors or State

Agencies being unaware of the requirement for collection of information, as State agencies are responsible for submitting the information they collect on their vendors into FDP.

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?

FDP contains information on WIC vendor management activities, not specific individuals.

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

FDP contains information on WIC vendor management activities, not specific individuals. State agencies have access to their data and are responsible for correcting any inaccurate or erroneous information that they have submitted into FDP.

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

FDP contains information on WIC vendor management activities, not specific individuals.

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

FDP contains information on WIC vendor management activities, not specific individuals.

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

FDP contains information on WIC vendor management activities, not specific individuals.

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?

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.

8.2 Will Department contractors have access to the system?

Yes. Information housed within FDP can be shared with agency contractors, grantees, experts, consultants or volunteers who have been engaged by the agency to assist in the performance of a service related to FDP and who need to have access to the records in order to perform the activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 USC 552a(m).

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

Users will access FDP by utilizing their USDA eAuthentication account. USDA requires all users who have an eAuthentication account to complete annual Information Security Awareness training, which includes modules on privacy training.

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

FDP is being added to the FNS Salesforce boundary, which has a current Authorization to Operate (ATO). The FNS Salesforce ATO will be updated in January 2021, following the completion of an independent assessment of the security and privacy controls for the solution.

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

FDP has auditing measures in place which can help diagnose potential or real security issues. It is recommended that ISO perform regular security audits to detect potential abuse. FDP can perform regular audits of Record Modification Fields, Login History, Field History Tracking, and Setup Audit Trail.

FDP utilizes a robust collection of technical safeguards to ensure the integrity of the platform. FDP is hosted in a secure server environment that uses a firewall to prevent interference or access from outside intruders. When accessing FDP, Secure Socket Layer (SSL) technology protects the user's information by using both server authentication and data encryption. FDP 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 FDP are stored in a privately owned data center with strict physical access control procedures in place to prevent unauthorized access.

8.6 Privacy Impact Analysis: 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?

The privacy risks associated with FDP are centered around the unauthorized disclosure of the personally identifiable information (PII) hosted on the platform. FDP utilizes 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 FDP features. Access to FDP is also tightly controlled through the use of eAuthentication and least role privileges.

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?

FDP is a data collection and reporting system that allows State agencies to export the State's WIC system of record results to the federal WIC Program. The development of FDP is a re-platform of the existing TIP system to the Salesforce Cloud that also enhances the functionalities currently provided by TIP system. The re-platform and enhancements will improve the Program's oversight capabilities.

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

No. FDP does not employ technology that will raise privacy concerns.

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?

The Agency does not use 3rd party websites or applications to operate FDP.

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

The Agency does not use 3rd party websites or applications to operate FDP.

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

The Agency does not use 3rd party websites or applications to operate FDP.

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?

The Agency does not use 3rd party websites or applications to operate FDP.

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

The Agency does not use 3rd party websites or applications to operate FDP.

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

The Agency does not use 3rd party websites or applications to operate FDP.

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?

The Agency does not use 3rd party websites or applications to operate FDP.

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)?

The Agency does not use 3rd party websites or applications to operate FDP.

10.10 Does the system use web measurement and customization technology?

FDP will not utilize web measurement or customization technology.

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?

FDP will not utilize web measurement or customization technology.

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.

The Agency does not use 3rd party websites or applications to operate FDP.

Agency Responsible Officials

MARCI GIORDANO
Digitally signed by MARCI GIORDANO
Date: 2020.11.30 09:44:32 -05'00'

Marci Giordano
FNS OIT Project Manager
Program Integrity and Monitoring Branch
Food and Nutrition Service
United States Department of Agriculture

Date

KELLY JACKSON
Digitally signed by KELLY JACKSON
Date: 2020.11.23 09:22:51 -05'00'

Kelly Jackson
Information Owner
Program Integrity and Monitoring Branch
Food and Nutrition Service
United States Department of Agriculture

Date

JOSEPH SHAW
Digitally signed by JOSEPH SHAW
Date: 2020.11.30 09:57:51 -05'00'

Joseph Shaw
System Owner
Food and Nutrition Service
United States Department of Agriculture

Date

Agency Approval Signature

JOSEPH BINNS
Digitally signed by JOSEPH BINNS
Date: 2020.12.01 09:08:08 -05'00'

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

Date