Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: June 17, 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

FNS Financial Management General Support System (FNS FM-GSS)

June 17, 2020

Contact Point

Sonja Farrell
Information System Owner
United States Department of Agriculture
703-305-2275

Reviewing Official

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

Abstract

This document is a Privacy Impact Assessment (PIA) for the FNS Financial Management General Support System (FNS FM-GSS). FNS FM-GSS includes subsystems and applications that the Agency leverages to gather, process, and report on financial data. The FM-GSS includes the financial applications and supporting platforms, which are hosted within the Microsoft (MS) Azure FedRAMP cloud environment. The PIA is being completed due to a Privacy Threshold Analysis (PTA) that indicated a PIA was required for the following subsystems located within the FNS FM-GSS ATO boundary: the Financial Management Application Toolset (FMAT) and the Grants Information Management System (GIMS).

Overview

The FNS FM-GSS includes the financial applications and supporting platforms, which are hosted within the Microsoft (MS) Azure FedRAMP cloud environment.

MS Azure FedRAMP is a Government FedRAMP approved cloud environment hosted in geographically-distributed MS Azure datacenters within the U.S. and is built on platforms implementing robust and scalable architectural standards. Azure provides several security controls, including, but not limited to border protection mechanisms, a redundant DNS architecture, and physical security protections. The established Digital Infrastructure Services Center (DISC) Azure tenant and the Cloud Service broker, is a representative for the United States Department of Agriculture (USDA) in Azure Active Directory, enables a Departmental managed approach to common controlled services for any agency opting to use Azure Government. DISC maintains a security system, and related technical services named the USDA Azure Cloud System, in which the GSS inherits. The FNS FM-GSS establishes and maintains its Azure subscriptions within this tenant that defines the basic boundary of the FNS FM-GSS.

The FNS FM-GSS ATO boundary includes the following subsystems covered under this PIA.

Financial Management Application Toolset (FMAT)

FMAT is a Financial Management Support Solution that includes web-based custom-designed applications residing on the FNS intranet. It is comprised of the following applications:

- **Automated Entity Resolution and Optimization System (AEROS)** is a custom solution providing the repository and mechanism for users to identify and match incoming collections to the appropriate customer and accounts receivable (AR) document. It provides a user interface for AR processors to view AR and collection-related data gathered from various systems, confirm data matches made by the system, and track and report on the status of collections throughout their lifecycle.
- **Budget User Desktop Solution (BUDS)** is an internal FNS web-interface module that provides a process-driven SF-132 budget execution tool for end-users. BUDS enables end

users to post SF-132 accounting events to the sub-allotment level and presents data in a user-friendly graphical interface.

- **Integrated Data Extraction and Analysis (IDEA)** is a user-definable data extraction and analysis tool to supplement the existing reporting and analysis capabilities of FMAT. The primary objective of this application is to automate the data extraction and validation processes of financial data.
- **Grant Award Document and Letter of Credit (GAD/LOC) Amendments Process (GLAP)** provides FNS grantees with an Adobe Portable Document Format (PDF) version of their GAD/LOC amendments. The reports have been electronically signed and dated by an authorized FNS employee in the Financial Management Modernization Initiative (FMMI).
- The **FMAT Interface Module** supports the exchange of data between BUDS, IDEA, AEROS, GLAP, and the FMMI.

Grants Information Management System (GIMS)
GIMS is a Document Management product that facilitates the management of all types and formats of content. It provides a secure, central repository for organizing and sharing content in an enterprise-wide fashion. It includes a flexible and powerful metadata categorization to enrich content by structured data in order to create custom properties, control document status, and support content search and retrieval. GIMS also has the capability to check-in/check-out documents; manage version control for simple and compound documents; track audit trails; perform comprehensive searches; and manage user, group, and role-based access controls.

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?

The information that is collected, used, disseminated or maintained in FNS FM-GSS is related to FNS programs applications The FNS FM-GSS may collect information which could include data from grants program which requires the FNS Request for Application (RFA), and data received via applications which the FNS System is externally connected There are forms such as SF-424, SF-424A, SF-LLL, Farm to School coversheet, which are processed by the system and also other additional information related to other FNS FM-GSS applications are collected and maintained. Additionally information entered by approved FNS FM-GSS users are maintained in the GSS. Examples of this information may include the applicant's employment history, key personnel salary data, or key personnel legal name, and address as well as pre-award, award and post-award details.

The information that is collected, used, disseminated or maintained in FMAT is specifically related to vendors maintained in the Financial Management Modernization Initiative (FMMI) system. This information may include the vendor's name, address, email IDs, and SSN/TIN.

The information that is collected, used, disseminated or maintained in GIMS is specifically related to FNS discretionary grant programs. This may include the FNS Request for Application (RFA), as well as data received via the Grants.gov download of application forms such as SF-424, SF-424A, SF-LLL, and Farm to School coversheet, and any additional documents provided by grant applicants. In addition, information entered by approved GIMS users to maintain official grant files is maintained in GIMS. This information may include the applicant's employment history, key personnel salary data, or key personnel legal name, SSN, handwritten signatures, Grants.gov user ID, and address as well as pre-award, award and post-award details.

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

The data sources for FNS FM-GSS are sourced through the applications hosted in FNS FM-GSS and transferred to connecting systems that process such data. Also other sources of data are entered by USDA FNS employees who have been approved for FNS FM-GSS access.

The data sources for FMAT include the following: (1) vendor data from FMMI; collection extract from Treasury's Collections Information Repository (CIR) system; and check images from Treasury's Electronic Check Processing (ECP) system.

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

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

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

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

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

1.4 How is the information collected?

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

FMAT also receives daily downloads from FMMI and the Treasury CIR & ECP systems, which is then uploaded into an encrypted database.

1.5 How will the information be checked for accuracy?

FNS FM-GSS downloads "Validated" Data from externally connected applications" and check for accuracy once received. Transmission integrity is provided by SSH-2. SSH-2 which uses cryptographically strong Message Authentication Code (MAC) algorithms to provide integrity and data origin assurance.

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

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

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

This process is driven by privacy laws, regulations, and government requirements, including the following:

Privacy Act (5 U.S.C. 552a(e));
e-Govt. Act, Sec. 208(c) (44 U.S.C. 3501);
Office of Management and Budget (OMB) Circular A-130;
Department Regulation 3515-002;
Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)

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

The recipient mailing address and financial data confidentiality risks are mitigated using logical access controls, physical access controls to GIMS, and personnel security controls. PII data not used for grants processing will be deleted and will not be stored in the GIMS database. PII data used for grant processing will be encrypted when before archiving, before transmission, and in primary storage (i.e., the archive server). A notification will be included in the display when displaying PII.

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

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

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

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.

The data in GIMS is being used to support the discretionary grants award process at FNS. This information is used to establish grant opportunities, receive applications, distribute applications for review, determine award and funding decisions, generate awards, maintain official grant file documentation and activities throughout the life of an award. The information is also used for reporting purposes to both internal FNS users, as well as external reporting as approved by the Grants Director.

FMAT receives payment collections data from Treasury and it uses FMMI to match the existing vendor information or create a new vendor in order to process the collection document.

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

Various software applications are utilized within FNS FM-GSS to access, analyze, and process data for reporting. For example, OpenText xECM for SAP, OpenText WebReports, and Microsoft Excel are used by GIMS to generate reports. Data that may be produced by GIMS includes the following:

- Application data contained within the standard federal forms including SF-424, SF-424A, , Farm to School coversheet and SF-LLL
- Financial data related to application budget detail and revisions, award funding, indirect costs and cost sharing/matching
- Grantee and organization information, such as DUNS number, points of contact, phone numbers, email addresses
- Application and award information such as eligibility, application/award status, award start/end dates, and property information
- Notes and comments as recorded in GIMS by FNS users

The data referenced above may be included in the following GIMS reports:

- Application Tracking Report (SF-424)
- Award Tracking Report
- Budget Tracking Report (SF-424)
- Grant Program Summary Report

FMAT uses Python based custom application to match the payer information from the Treasury system with possible matches on the FMMI system, using their name, address, case number etc. This logic is used to determine the vendor against which the collection will be processed. In case of no matches, the system will use the information to create a new vendor to process the collections.

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

Not applicable. FNS FM-GSS applications do 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.

Logical access controls, physical security controls, and personnel security controls are used to limit access to GIMS PII data based on least privileging and a need-to-know. OpenText xECM for SAP permissions to access data and execute OpenText xECM functionality are assigned to user roles.

The OT archive server and database will encrypt all data. Data will be encrypted before transmission from or downloading from the GIMS.

Certificate-based Mutual Authentication is used to gain access to grants.gov and the data transmission is encrypted using SSH-2

Logical access controls, physical security controls, and personnel security controls are used to limit access to FMAT PII data based on least privileging and a need-to-know.

The FMAT database will be encrypted along with the files received from Treasury. The FMMI files are deleted after they are loaded on to the database.

All PII data is being masked in the database and only users with PII privileges will be able to view it. None of the users will have access to modify any PII data.

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?

GIMS information is retained and archived in primary storage for six (6) years after the closeout of the program and archived per FNS archival policy. FMAT information is retained and archived in primary storage for six (6) years after final Payment or cancellation.

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

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

Access to computerized files is password protected and under the direct supervision of the system manager. Data will be maintained based on the identification records retention for the specific data types for FNS FM-GSS applications.

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

Data is retained and archived in GIMS and FMAT for a period of six (6) years and is encrypted in backup storage and primary storage. Any risks associated with the length

of time is mitigated via data encryption. Archived data is encrypted in accordance with the FNS policies.

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?

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

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

4.2 How is the information transmitted or disclosed?

The information created by FMAT is used to manually create Vendor records in FMMI.

The information as noted in 4.1 may be disclosed electronically via an Excel, Word, PDF document, or via hard copy. It could be data from GIMS or standard GIMS reports. Transmissions/disclosures typically require approval by the Grants Director.

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.

Access to FNS FM-GSS applications is authorized by the application Account Managers, identified by the System Owner. Data will be shared with external audiences per the System Owner's discretion and approval.

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?

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

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.

Applications within FNS FM-GSS are covered by SORN FNS-10, Persons Doing Business with Food and Nutrition Service (FNS). Sharing of PII is limited to review panelists involved in the grants process. Application systems will redact received EIN/TIN from applications. Other PII will be encrypted before distributing to review panelists. The PII is not used as a key for tracking, as a primary key, or foreign key to identify an individual.

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

The encrypted PII may be disclosed electronically via an Excel, Word, PDF document, or via hard copy. It could be data from GIMS or standard GIMS reports. Transmissions/disclosures typically require approval by the Grants Director.

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

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

Section 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, a SORN is required for GIMS. The SORN is used from the originating source Grants.gov

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

Privacy Statement is provided in the Privacy Policy section of the Request for Applications (RFAs). Applicants responding to FNS RFA via Grants.gov are required to complete the federal forms which may contain PII data. FNS downloads this information into GIMS via the Grants.gov interface on the application deadline as published in the RFA on Grants.gov.

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

Applicants responding to an FNS RFA via Grants.gov are required to complete the federal forms which may contain PII data. If an application does not include all appropriate information, as noted in the RFA, FNS will consider the application to be non-responsive and will eliminate it from further evaluation.

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

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

Applicants who are responding to the FNS Request for Applications (RFAs) are required to complete the federal forms which may contain PII data. Applicants can also submit additional attachments. At an applicant's option, they could submit a notification regarding the right to consent to particular uses of the information.

GIMS uses Grants.gov managed by the Department of Health and Human Services. Grants.gov provides a common website for federal agencies to post discretionary funding opportunities and for grantees to find and apply to them.Grants.gov provides a privacy policy on their website, accessible here: https://www.grants.gov/web/grants/privacy.html?inheritRedirect=true

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.

The Notice is provided in the REQUEST FOR APPLICATIONS (RFA) under the section "**Safeguarding Personally Identifiable Information**" as follows.

Safeguarding Personally Identifiable Information
Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (National Institute of Standards and Technology (NIST) SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable information, April 2010).

Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records, and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (National Institute of Standards and Technology (NIST) SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable information, April 2010).

Applicants submitting applications in response to this RFA must recognize that confidentiality of PII and other sensitive data is of paramount importance to the USDA Food and Nutrition Service. All federal and non-federal employees (e.g., contractors, affiliates, or partners) working for or on behalf of FNS are required to acknowledge understanding of their responsibilities and accountability for using and protecting FNS PII in accordance with the Privacy Act of 1974; Office of Management and Budget Memorandum M-06-15, *Safeguarding Personally Identifiable Information; M-06-16, Protection of Sensitive Agency Information*; M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; and the NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information*.

By submitting an application in response to this RFA, applicants are assuring that all data exchanges conducted throughout the application submission and pre-award process (and during the performance of the grant, if awarded) will be conducted in a manner consistent with applicable Federal laws. By submitting a grant application, applicants agree to take all necessary steps to protect such confidentiality, including the following: (1) ensuring that PII and sensitive data developed, obtained or otherwise associated with UDSA FNS funded grants is securely transmitted. Transmission of applications through Grants.gov is secure; (2) ensuring that PII is not transmitted to unauthorized users, and that PII and other sensitive data is not submitted via email; and (3) Data transmitted via approved file sharing services (WatchDox, ShareFile, etc.), CDs, DVDs, thumb drives, etc., must be encrypted.

Section 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?

FMAT is not the system of records as the Vendor PII information is captured either through FMMI or Treasury systems. So any data corrections required by the individual will be addressed by the corresponding systems.

Individuals do not have access to information in GIMS once their applications have been downloaded into GIMS via Grants.gov.

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

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

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

Applicants are notified via the RFA, as posted in Grants.gov, that FNS will not consider additions or revisions to applications after the application deadline in Grants.gov.

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

None.

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

None.

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?

A FMAT Access Request Form is required to create, modify or delete access to AEROS and must be approved by the Supervisor and the System Security Administrator. Users are set up by adding them to Windows AD group AFNG_AR and assign roles.

A GIMS Access Request Form is required to create, modify or delete access to GIMS and must be approved by the by the Supervisor and the System Security Administrator. Users are set up by adding them to Windows AD group AFNG_OTUsers_Group. and OpenText xECM group membership.

8.2 Will Department contractors have access to the system?

Yes, FNS contractors have access to the FNS FM-GSS applications for the following reasons:

- Retrieval and upload of Grants.gov files;
- Back-Up of files and data;
- Application and database support;
- Account management; and
- Operating system support.

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

USDA FNS privacy training is provided to FNS FM-GSS users and support personnel.

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

The FNS FM-GSS received an Authorization to Operate for three (3) years in June 2019 and is currently undergoing the A&A process for FY20.

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

OpenText xECM folder permissions, role-based access control, database encryption, data masking, and audit trail capabilities are implemented to prevent misuse of data.

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 identified are related to the employer identification number (EIN) or the taxpayer identification number contained in GIMS. This PII data will be stored in an encrypted database once grant application files are downloaded from Grants.gov.

As referenced in Section 2.3, the other information collected in GIMS is as follows:

- Application data contained within the standard federal forms including SF-424, SF-424A, Farm to School coversheet, and SF-LLL
- Financial data related to application budget detail and revisions, award funding, indirect costs and cost sharing/matching
- Grantee and organization information, such as DUNS number, points of contact, phone numbers, email addresses
- Application and award information such as eligibility, application/award status, award start/end dates, and property information
- Notes and comments as recorded in GIMS by FNS users

This information is not considered PII. GIMS users will be instructed to notify the Grants Director if they identify additional risk of PII, at which time a procedure for redacting the PII can be determined.

The information that is collected, used, disseminated or maintained in FMAT is related to Vendors maintained in the FMMI system. This information may include the vendor's name, address, email IDs, SSN/TIN, Check images along with signatures, bank Account numbers & bank routing numbers.

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

The FMAT database will be encrypted along with the files received from Treasury. The FMMI files are deleted after they are loaded on to the database.

All PII data is being masked in the database and only users with PII privileges will be able to view it. None of the users will have access to modify any PII data.

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?

FNS FM-GSS is a General Support System.

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.

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

Not applicable.

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.

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.

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

Not applicable.

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.

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.

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.

10.10 Does the system use web measurement and customization technology?

Not applicable.

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 <u>Privacy Impact Analysis</u>: 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.

Responsible Officials

SUBATHRA ILANCHEZHIAN
Digitally signed by SUBATHRA ILANCHEZHIAN
Date: 2020.06.18 15:35:18 -04'00'

Suba Ilanchezhian
Project Manager
Food and Nutrition Service
United States Department of Agriculture

Date

SONJA FARRELL
Digitally signed by SONJA FARRELL
Date: 2020.06.19 12:03:29 -04'00'

Sonja Farrell
Information System Owner
Food and Nutrition Service
United States Department of Agriculture

Date

Approval Signature

JOSEPH BINNS
Digitally signed by JOSEPH BINNS
Date: 2020.06.22 10:59:05 -04'00'

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

Date