Privacy Impact Assessment

Financial Processing Center General Support System (FPC-GSS)

Version: 13.0
Date: April 4, 2023
Prepared for: Food Safety and Inspection Service (FSIS)

Privacy Impact Assessment for the FPC-GSS

April 4, 2023

Contact Point

Christine Turner (System Owner)
Office of Chief Financial Officer (OCFO)
Office of the Administrator (OA)
Food Safety and Inspection Service (FSIS)
United States Department of Agriculture (USDA)
301-837-7718

Reviewing Official

Timothy Poe
Privacy Officer
202-205-3828
United States Department of Agriculture

Revision History

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
3.0	03/21/2014	Rachel Gardezi	Converted to New Template and provided review for 2014
4.0	11/13/2014	Erik Nudo	Annual Update for 2015
4.1	12/22/2014	Erik Nudo	Review complete by System Owner
4.2	4/1/2016	Erik Nudo	Annual Review
4.3	7/19/2016	Erik Nudo	Review and Signature from System Owner
4.4	7/22/2016	Erik Nudo	Review and Signature from CISO
4.5	8/1/2016	Erik Nudo	Review and Signature from CIO
5.0	8/1/2016	Erik Nudo	Review and Signature from FSIS Privacy Office and Finalize
5.1	10/20/2016	Erik Nudo	FY17 Annual Review
6.0	03/13/2017	Tope Ayodeji	Annual Review for 2017
6.1	03/14/2018	Tope Ayodeji	FY18 Annual Review
7.0	09/06/2018	Kathryn Stuart	Finalized Document at Conclusion of FY18 Assessment
7.1	01/23/2019	Kathryn Stuart	FY19 Annual Review and Update for ATO Renewal
7.2	02/12/2019	Kathryn Stuart	Finalized updates from FY19 update- prepared for signature and privacy office review.
8.0	07/08/2019	Kathryn Stuart	Finalized document after all signatures received for FY19 ATO

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
8.1	01/08/2020	Kathryn Stuart	FY20 Annual Review
9.0	07/02/2020	Kathryn Stuart	Finalized document at conclusion of FY20 A&A cycle
9.1	10/15/2020	Trang Nguyen	Updated section 7.0 to address POA&M 30553
9.2	11/23/2020	Trang Nguyen	Updated section 6.4 to address POA&M 30554
9.3	11/24/2020	Trang Nguyen	Updated section 6.4 to address SCA's feedback
10.0	02/02/2021	Trang Nguyen	CY21 Annual Review and Update
11.0	03/23/2022	Trang Nguyen	CY22 Annual Review and Update
11.1	06/23/2022	Trang Nguyen	Removed Privacy Officer's name and information per new direction from the Dept. Privacy team
11.2	07/11/2022	Trang Nguyen	Minor updates to address Privacy team's feedback
12.0	01/03/2023	Trang Nguyen	CY23 Annual Review and Update
13.0	04/04/2023	Trang Nguyen	Tableau Integration Update

**NOTE:* *During Annual Assessment, the System Owner and/or Information System Security Officer (ISSO) Representative reviews this Privacy Impact Assessment (PIA). A Revision number is identified in the table to represent this annual review, although no document signatures are required unless significant system/organizational document changes are involved.*

Abstract

This document serves as the Privacy Impact Assessment for the Financial Process Center- General Support System (FPC-GSS). The purpose of the system is to provide information, processing, and analysis of financial documents that represent multi-million-dollar receivables and payments to employees and vendors in support of FSIS. This assessment is being done in accordance with the Privacy Threshold Analysis (PTA) conducted in 2023.

Overview

The United States Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) Financial Processing Center- General Support System (FPC-GSS), is responsible for the entry, verification, authorization, processing, and document management of payroll, travel, billing, collections, debt management, and miscellaneous payments. The FPC-GSS was created in late 1996 as part of the administrative consolidation of FSIS. As the FSIS national center for data processing and financial services, it supports approximately 9,500 – 10,000 permanent and 500 – 1,500 temporary Agency employees throughout the United States. The FPC-GSS provides financial information in various formats to the offices throughout the Agency and responds to inquiries and audits upon request. Re-establishment is underway to allow FPC-GSS domain connection to the PolyBase environment, then PolyBase will connect to Tableau environment. This connection between FPC-GSS and PolyBase will share various data from FPC-GSS for analysis and reporting purposes.

FPC-GSS receives USDA FSIS employee Social Security Numbers (SSNs) from the National Finance Center (NFC), which were originally provided to the NFC by USDA FSIS, along with other employee payroll and travel data.

Also, the FPC-GSS processes and issues summary reports for processing of egg products for the FSIS Policy Development Division (formerly the Technical Service Center (TSC) within Office of Policy Program Development (OPPD) and USDA National Agricultural Statistics Service (NASS).

The FPC-GSS is the electronic repository for all FPC-GSS processed Time and Attendance (T&A), Travel Vouchers, Miscellaneous Pay and the Agency form 5110s (to record reimbursable charges).

For inputs into the FPC-GSS, authorized users located in Urbandale, process the data received from employees' electronic format and data received from the NFC, which is manually fed into the FPC-GSS daily. The system administrators within the FSIS Office of the Chief Information Officer (OCIO) control the access levels for the FPC-GSS.

FPC-GSS is part of the Microsoft Cloud fabric under the Azure Network General Support System (Azure N-GSS) boundary which provides Internet service to the public and private (Intranet) service to FSIS employees. The public does not authenticate to any portion of FPC-GSS and only FSIS employees with a PIV card can access the FSIS Intranet. FPC-GSS is connected to the Internet to serve public Web pages; however, it is protected by USDA firewalls. FPC-GSS is not located in a harsh environment that would be detrimental to the hardware or to the system's performance and availability.

The FSIS Azure Network General Support System (Azure N-GSS) provides the network, server

hardware, and operating system components of the system. The applications, data components and physical site are covered as part of the Security Assessment and Authorization (SA&A) effort.

The FSIS Azure N-GSS supports assigned authorizations for controlling the flow of information to facilitate data/information exchange through the use of Active Directory (AD), the application firewall Access Control Lists (ACLs), the use of encryption devices such as Virtual Private Networks (VPNs), and the use of encryption protocols, such as Secure Sockets Layer (SSL) and Internet Protocol Security (IPSEC), to support a secure connection.

FPC-GSS system administrators supervise user activities regarding the use and the application of information system access controls. The administrators utilize automated controls and mechanisms that support and facilitate the review of user activities. The FPC-GSS also enforces separation of duties through distinct user roles and groups to which the users are assigned. For system administrators, FPC-GSS ensures that individuals who are responsible for security do not also administer access controls or audit security logs. The details of Access Control are in the FPC- GSS System Security Plan (SSP) and Access Control (AC) Standard Operating Procedure (SOP).

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 FPC-GSS collects data that may include employee and customer/vendor names and addresses, business addresses, resident mailing addresses, as well as employee salary and grade. The different types of information collected, used, disseminated and maintained are within various components of the FPC GSS. The following lists the components and their uses:

Financial Services Consolidated Operations Management (FSCOM) / sFTP / SQL database FICFODM

Data Collection Fields: SSN, name, duty station information, program area, series, grade, step, salary, home address, demographic data, vendor number, pseudo code, establishment number, name, DBA, address information, Tax Identification Number (TIN), customer number, contact information (name, phone, email), PP covered, Transaction Code (TC) Prefix, TC, TC Suffix, name, timekeeper, year, Accounts Payable (AP), accounting code, work hours, Annual Leave (AL)/Sick Leave (SL), schedule, appointment, city, state.

Use: Data is received from NFC on a bi-weekly basis and PHIS on a daily basis. The data is used for various internal FPC-GSS tasks for processing and validation purposes (payroll, awards, billing, payments, debt management, etc.)

The System is used to receive payroll and employee information from the NFC mainframe to provide a means of creating a multitude of reports that provide various FSIS Branches statistical data. This data assists them in managing employee work hours and their budgets. The data is maintained in the database.

Information is pulled from NFC to the FICFODM database; this is used only for special mailings and in response to security check inquiries. The salary information is used for reports that summarize totals, but do not report specific employee salary data.

Customer information is captured. Ordinarily, the information is captured via submitting scanned copies of documents through e-mail or faxing of documents. The PII data include: Taxpayer Identification Number, Name, and Billing Location, Phone, Fax, and e-mail; however, information can also be captured by contacting a customer via phone when needed and typing the information into the system.

The FPC-GSS collects employee SSNs from NFC. FPC uses the SSN as a unique identifier to merge data into a report, but this report does not include the SSN in the

final output that is sent to the various FSIS district offices and Headquarters. As part of this processing, FPC-GSS also calculates the amount to be reimbursed to the establishment. Any information regarding reimbursement is correlated internally within this specific component and sent to NFC directly for payment. There are no PII outputs for individuals. These outputs apply only to establishments and are for establishment reimbursement purposes only. Internal system associations match the individual to the hours worked and the establishment; this internal process allows for the individual to be paid without any additional outputs.

Additional precautions are taken to ensure proper handling of PII, which include the SSNs display in truncated form based on user roles. User roles and responsibilities are defined in the FPC-GSS AC SOP and SSP. When the report is finalized and sent outside of FPC-GSS, the SSNs are redacted. Once the SSN is confirmed to be accurate for a specified employee, the system automatically displays personnel data for viewing without displaying the SSN. Finally, all of this data is encrypted when it is stored and access to the information system components is highly restricted.

Gimmal

Data Collection Fields: Billing Document (BD) number , EmplID, vendor code/Customer number, timekeeper, Pay Period (PP), Fiscal Year (FY)/Calendar Year (CY).

Use: Used to maintain image files of all employee timesheets and billing documents. This system gives FPC employees the ability to immediately view images of timesheets to answer employee questions and/or billing documents (5110's) to respond to plant requests. This database is also used to research time and attendance or billing corrections.

Tableau Integration

Tableau will not collect data, instead it will access the data already collected and available on FICFODM database (see SQL above).

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

FPC-GSS receives USDA FSIS employee SSNs from the NFC, which were originally provided to the NFC by USDA FSIS, along with other employee payroll and travel data. There is secure communication between NFC and the FPC-GSS, using tools such as TN3270 and sFTP.

Customer (vendor) information (Taxpayer Identification Number, Name, and Billing Location, Phone, Fax, and e-mail) is captured by contacting the customer when needed and having them submit establishment information via scanning and mailing or faxing information to FPC. All FPC-GSS data are encrypted in transit and at rest. Communications are Secured Socket Layer (SSL) through SSL encryption.

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

The information in the FPC-GSS is used for payroll and benefits management and to process billing and reimbursements. The information collected is used for these processes and for reporting on these processes.

1.4 How is the information collected?

The data is fed from the Department employee payroll programs into the FPC-GSS. Data is entered into the system by the individual employee and customer. For customer accounts information, the customer is contacted directly. Customer information (Taxpayer Identification Number, Name, and Billing Location, Phone, Fax, and e-mail) is captured by the FPC when needed, by having the customer submit establishment information via scanning and mailing or faxing information to FPC.

1.5 How will the information be checked for accuracy?

The originating system has already made accuracy checks prior to importation into FPC. However, the FPC-GSS periodically pulls the data for validation and to ensure proper report generation. FPC-GSS utilizes the payroll SSN to reconcile payroll hours worked and reimbursable hours charged to report any variance per Office of Inspector General (OIG) audit. In other words, a cross reference between employee names and SSNs is done to ensure accuracy and integrity.

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

The authorities for USDA to collect, maintain, use and disseminate information through this system are: 5 U.S.C.301 (government organization and employees); Title 5 USC 552a (Records Maintained on Individuals (Privacy Act)); Title 41 CFR 201-6.1 (Federal Information Resources Management Regulation); 44 U.S.C.3101 (Records Management); OMB Circular No. A-108 (Responsibilities for the Maintenance of Records About Individuals by Federal Agencies); OMB Circular No. A-130 (Management of Federal Information Resources, Appendix 1, Federal Agency

Responsibilities for Maintaining Records About Individuals); and Authorization to Operate (ATO), dated 07-15-2019.

In addition, USDA is generally authorized to collect information to support its mission under: Title 7, Chapter 55-2205 (7 U.S.C 2204) (which authorizes the Secretary of Agriculture to collect information and employ any sampling or other statistical method deemed appropriate); 21 U.S.C. 679c(a)(1)-(3) (which expressly authorizes the Secretary to give high priority to enhancing the ability of FSIS to conduct its mission); the Federal Meat Inspection Act (FMIA) (21 U.S.C. 601, et seq.), the Poultry Product Inspection Act (PPIA) (21 U.S.C., et seq.), the Egg Products Inspection Act (EPIA) (21 U.S.C. 1031, et seq.), and the Humane Methods of Livestock Slaughter Act of 1978 (7 U.S.C. 1901-1906).

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

The primary risk is that FSIS employee SSNs or other PII would be made available to unauthorized users or used for unauthorized purposes.

Risks to privacy are mitigated by granting access only to authorized persons. All USDA employees have undergone a background investigation. All FSIS employees must complete the annual security awareness training to maintain FSIS computer network account access. SSNs are redacted or truncated in reporting, further mitigating risk.

There are firewalls and other security precautions in place. For example, all authorized staff using the system must comply with the Agency's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III. All security controls in the system are reviewed when significant modifications are made to the system, and at a minimum, every 3 years. Active Directory and FPC-GSS role-based security are used to identify the users authorized for access and having a restricted set of access.

Access to facilities is typically controlled by Departmental security system, and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel.

Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad-hoc monitoring of computer usage.

If FPC-GSS employees need to send data to NFC via e-mail, there are controls in place to ensure the data is encrypted. The document with the PII information is saved with a special password that only the FPC-GSS requestor and NFC security know to open the document. Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect or incomplete data as recorded in the system. Any

contractors who may be authorized to access the system (e.g., Software (SW) developers) are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel who are expert in such matters.

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 FPC-GSS provides financial information in various formats to offices throughout the Agency and responds to inquiries and audits upon request. The following lists the FPC GSS components that handle PII and their uses:

FSCOM/sFTP/FICFODM- Data is received from NFC on a bi-weekly basis and PHIS on a daily basis. The data is used for various FPC tasks for processing and validation purposes (payroll, awards, billing, payments, debt management, etc.). The NFC Data includes payroll information from the NFC mainframe to provide reports and statistical data for various FSIS offices. This data assists in managing employee work hours and the office budgets. The data is maintained in a database and several other databases are linked to tables within the Pay Data System. PHIS data is used for the processing of billing for export application submissions. This information includes the establishment information, export countries, species listed on application, submitted name, email, phone and time of submission.

Any audit reports that would contain PII are redacted and filtered as appropriate. The original reports never leave the government property.

The use of SSN in the FSIS FPC-GSS is necessary because it is a unique identifier that FPC-GSS uses to pull data, produce reports, and reimbursements. The SSN is also used to ensure proper supporting documentation is provided for case reviews and OIG audits.

Gimmal - Used to maintain image files of all employee timesheets and billing documents. This system gives FPC employees the ability to immediately view images of timesheets to answer employee questions and/or billing documents (5110's) to respond to plant requests. This database is also used to research time and attendance or billing corrections,

Tableau Integration - PolyBase communication will be established with FPC-GSS to transmit data for the use of Tableau for analysis and reporting.

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

There are no external tools used for FPC-GSS data retrieval and analysis. The FPC-GSS uses select search criteria in order to filter and analyze the data to ensure the correct employee is identified when there are name duplications. The search criteria used is the employee SSN, employee name and employee location. The search and

analysis are conducted online on an FSIS laptop and printed in a hardcopy report.

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

The system does not use commercially or publicly available data. All data related to vendors or establishments is obtained directly from the vendor or establishment entity.

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.

System managers are charged with regulating access to computerized files that are password-protected and under the direct supervision of the system manager. The system manager has the ability to print out audit trails of access to the computer applications, thereby permitting regular ad-hoc monitoring of computer usage.

To mitigate the risks of divulging individual SSN, the SSN is transferred from NFC to FPC-GSS via secure FTP (the traffic is encrypted). In addition, once the SSN is confirmed to be accurate for a specified employee, the system stores only the last four (4) digits of that employee's SSN. The SSN fragment is also encrypted when it is stored.

Access to facilities is controlled by security system and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel.

See Section 1.7 above for a description of the controls that have been put in place for FPC-GSS and the FSIS environment.

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?

Data in paper and electronic format is maintained until they become inactive per NARA requirements (over 6 years), at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the NARA.

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

Yes. The retention period is 6 years and 3 months for physical documents. FPC-GSS uses the NC 1-016-77-02 retention schedule.

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 length of time data is retained does not change the level or type of risk associated with retaining the data. Therefore, the same methods to reduce risk are used throughout the life of the data. The largest risk is that federal employee SSNs are collected and used in the FPC-GSS system. To mitigate the risks of using the SSN, the SSN is transferred from NFC to FPC-GSS via a secure FTP (the traffic is encrypted).

See Section 1.7 above for a description of the controls that have been put in place for FPC-GSS and the FSIS environment.

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?

The purpose of the FPC-GSS is to handle various processing and analysis aspects of payroll, travel, billing, collections, debt management, and miscellaneous payment. The information is shared in order to ensure personnel payroll records are processed properly, employees and vendors are reimbursed for travel expenditures, and the USDA is reimbursed for services it provides.

If special requests come from U.S. courts, LERD, Civil Rights, OGC, or OIG, information is redacted. In addition, SSN's are not shared with any other USDA organization.

4.2 How is the information transmitted or disclosed?

All employee specific data is pulled from NFC over a secure, encrypted line, set up by FSIS OCIO and USDA OCIO. Data never leaves FPC-GSS via downloaded data, only finished reports. In other words, FPC-GSS operates in a "one-way" pull into FPC-GSS. FPC-GSS can then produce the various financial reports for which they were created.

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.

SSNs are always redacted and never shared outside of the FPC-GSS office. Documents containing PII information that are requested and provided to any authorized entity (e.g., LERD, Civil Rights, OIG, the courts, etc.), will have SSNs redacted from the image provided. Privacy risk is low because access to data is strictly controlled. Access is granted through an approved process and authorization within FPC-GSS is role based to ensure least 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?

Generally, information is not shared with organizations external to the USDA.

If necessary, information may be disclosed to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to NARA or to the General Services Administration (GSA) for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to FSIS contractors pursuant to 5 USC 552a(m), for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised.

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.

Under normal circumstances, FPC-GSS does not share PII outside of the Department. However, routine use for disclosure is permitted to the Department of Justice for use in litigation, for disclosure to adjudicative body in litigation, law enforcement purposes, for disclosure to a Member of Congress at the request of a constituent, for disclosure to the NARA or to the GSA for records management inspections conducted under 44 USC 2904 and 2906, for disclosure to appropriate agencies, entities, and persons when the agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised. FPC-GSS is covered by Departmental SORN OP-1 (Personnel and Payroll System for USDA Employees).

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

Should FPC-GSS information need to be shared externally, departmental guidelines for providing information to such organizations will be followed. This includes the redacting of PII, unless the information is required under law.

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

As long as employee PII data is transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee PII is not shared externally. Such information would only be provided if required by law. Standard FSIS or USDA guidelines for protecting the information would be followed.

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. FPC-GSS does require a SORN and is covered by Departmental SORN OP-1 (Personnel and Payroll System for USDA Employees).

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

Yes. Notice is provided to the individual prior to collection of any information, in accordance with USDA Memorandum Minimum Safeguards for Protecting Personally Identifiable Information (PII) for all Source System users. Plant vendors are provided notification during business agreement processes.

The user is told prior to system access that entering their name is a requirement of working on the system; therefore, the user is notified.

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

Yes. However, the information is required as a condition of either employment or to do business with FSIS.

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

Yes. The privacy act notice statement is included on both the 5200-2 and W-9 forms which are provided to the users, so they understand their rights with regards to authorizing and consenting to the collection and use of their PII. Signed submission of the form indicates a user's consent to PII collection, use, and maintenance within FPC-GSS. If a user does not consent, which means he/she does not sign and submit the forms, then nothing is collected by the agency. The ramifications for not consenting are laid out on the 5200-2 and W-9 forms.

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.

There is no risk of individuals being unaware because information is being requested

directly from employees or companies.

See Section 6.1 above.

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?

Individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA office.

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 2166, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 720-2109 - Fax (202) 690-3023 – E-mail: fsis.foia@usda.gov.

For more information about how to make a FOIA request, please see:

http://www.fsis.usda.gov/wps/portal/footer/policies-and-links/freedom-of-information-act/foia-requests

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

If there is a complaint, concern, or question, FPC-GSS has a messaging mechanism through which customers can send complaints or requests to correct their PII or inaccurate/erroneous information. They can contact FPC-GSS at 1-800-949-3964 or email FSIS.Billing@usda.gov.

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

Before providing information, the individual is presented with a Privacy Act Notice and an explanation of the Notice, on both the Form 7234-1 and Form 8822-4. The individual's acknowledgement of the Privacy Act Notice and the proffer of information signify the individual's consent to the use of the information. The purpose, use, and authority for collection of information are described in the Privacy Act Notice.

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

N/A

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

There are limited privacy risks associated with redress. Data requested as part of redress is afforded the same level of protection as the original data. Redress will be handled primarily as specified above in Section 7.2.

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?

Windows Active Directory controls are used to prevent users from accessing information they are not authorized to use. All FSIS users are assigned a Windows Active Directory account once their credentials and need for access are verified. AC policy and procedures are documented in the AC SOP and further details of the AC specifications can be found in the FPC-GSS SSP.

All users are required to complete computer security training prior to accessing the system and must complete annual refresher training to retain access. Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

In addition, FPC employees are trained not to provide information via phone.

If FPC employees need to send data to NFC via e-mail, there are controls in place to ensure the data is encrypted.

8.2 Will Department contractors have access to the system?

Contractors may be authorized to access the system. Their use of the system is governed by contracts identifying rules of behavior for USDA and FSIS systems and security. In addition, the same AC policies and procedures apply to contractors, as well as government employees.

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

All users are required to complete computer security training prior to accessing the system and must complete refresher training in order to retain access.

In addition, FPC-GSS employees are trained not to provide information via phone. There is also a privacy component provided within the annual computer security training provided by USDA.

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

Yes, the Authority to Operate (ATO) was granted on July 15, 2019 and will be renewed in July 2022.

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

The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.

Once the SSN is confirmed to be accurate for a specified employee, the system displays personnel data for viewing without displaying the SSN. All of this data is encrypted when it is stored. The data is read-only and cannot be manipulated by users. Finally, reports are only outputted to the screen for visual verification, to ensure alignment with pay period. Aggregated data is produced from the system at this level.

The IT technical security safeguards are FIPS 200 and NIST SP 800-53 Rev.5.

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 risk is that personal information might be shared with individuals who should not have access to the information and who might misuse the information. Therefore, the FPC-GSS has mitigated these risks by granting access only to authorized persons. Further, all USDA employees have undergone a background investigation and contractor access is governed by contracts identifying rules of behavior for USDA and FSIS systems and security.

Authorized users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.

Access to facilities is typically controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel.

Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

If FPC-GSS employees need to send data to NFC via e-mail, there are controls in place to ensure the data is encrypted.

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?

FPC-GSS is a Major 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. Both M-10-22 and M-10-23 have been reviewed by the SO and ISSPM.

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

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

If so, is it done automatically?

N/A - Third party websites are not being used.

If so, is it done on a recurring basis?

N/A - Third party websites are not being used.

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

N/A - Third party websites are not being used.

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?

N/A - Third party websites are not being used.

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)?

N/A - Third party websites are not being used.

10.10 Does the system use web measurement and customization technology?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A.

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?

N/A.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A.

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.

N/A - Third party websites are not being used.

Responsible Officials

Christine Turner
System Owner
5601 Sunnyside Avenue
Beltsville, MD 20705

Marvin Lykes
Chief Information Security Officer (CISO)
1400 Independence Ave., SW
Washington, DC 20250

Carl A. Mayes
Assistant Chief Information Officer
1400 Independence Ave., SW
Washington, DC 20250

Approval Signatures

Agreed: _____ _____

Christine Turner — Date

System Owner

Agreed: _____ _____

Marvin Lykes — Date

Chief Information Security Officer (CISO)

Agreed: _____ _____

Carl A. Mayes — Date

Assistant Chief Information Officer