Privacy Impact Assessment

Financial Processing Center – General Support System (FPC-GSS)

- Version: *2.5*
- Date: *September 20, 2012*
- Prepared for: FSIS CFO

USDA

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
2.4	03/15/2012	Rachel Gardezi	Moved 2012 PIA to new template
2.4	06/20/2012	Rachel Gardezi	Integrated User Representative and Privacy Officer comments
2.4	08/03/2012	Victor Williams	Integrated information from business and security into document.
2.4	08/14/2012	Rachel Gardezi	Integrated Privacy Officer and User Representative comments
2.5	9/20/2012	Victor Williams	Updated to reflect changes to complete document

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 February 2012.

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.

There is secure communication between National Finance Center (NFC) and the FPC-GSS, using tools such as TN3270 and File Transfer Protocol (FTP). FPC-GSS receives USDA FSIS employee Social Security Numbers (SSNs) from the 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).

Processing Flow

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

The FSIS Network General Support System (N-GSS) and Enterprise General Support System (E-GSS) provide the network, server hardware, and operating system components of the system. The applications, data components and physical site are covered as part of the Certification and Accreditation (C&A) effort.

Security Protection

The FSIS N-GSS and E-GSS support 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.

Access Control

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 located 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:

FSIS Employee System

Data Collection Fields: SSN, name, duty station information, program area, series, grade and step
Use: Data is downloaded from NFC on a weekly basis. The data is used for various FPC research tasks for validation purposes (create labels, reports, etc.)

FSIS Vendor Search System

Data Collection Fields: App#, plant#, plant info, DBA, state, comments, vendor code, A database was created to keep track of vendors by app no, plant no and/or name.
Use: Allows the Accounts Receivable Branch to research plant billing information and to provide labels for the 5110s for scanning/filing purposes. It is also linked to other database for validation purposes.

Smead Imaging (TA/5110)

Data Collection Fields: Billing Document (BD) #, SSN, vendor code, timekeeper, PP, FY/CY,
Use: Used to maintain image files of all employee timesheets and billing documents. This system gives FPC Financial Technicians 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

NFC Pay Data System

Data Collection Fields: SSN, PP covered, PP processed, TC Prefix, TC, TC Suffix, name, timekeeper, year, AP, accounting code, work hours, AL/SL, schedule, appointment, city, state
Use: The NFC Pay Data System is used to download pay 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 a database and several other databases are linked to tables within the Pay Data System.

Information is pulled down from NFC for the FSIS Employee System; 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 for the FSIS Vendor Search System by the Smead Imaging (TA/5110) which supports the FSIS Vendor Search component by allowing customers to send scanned images of documents. Ordinarily, the information is captured via submitting scanned copies of documents thru email or faxing of documents. The PII data include: Taxpayer Identification Number, Name, and Billing Location, Phone, Fax, and email; however, information can also be captured by contacting a customer when needed and inputting the information via phone.

The FPC-GSS collects employee Social Security Numbers (SSN) from NFC Pay Data System. 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.

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 FTP.

Customer (vendor) information (Taxpayer Identification Number, Name, and Billing Location, Phone, Fax, and email) is captured by contacting the customer when needed and having them submit establishment information via scanning and mailing or faxing information to FPC

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 inputted 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 email) is captured by the FPC when needed by having them 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?

44 U.S.C. 3101 states that each USDA mission area, agency, and staff office shall create and maintain proper and adequate documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the Department of Agriculture (Department) to protect the legal and financial rights of the Government and of persons directly affected by the Department's activities.

US Code TITLE 7, CHAPTER 55 - 2204 states that the Secretary of Agriculture may conduct any survey or other information collection, and employ any sampling or other statistical method, that the Secretary determines is appropriate. USDA is also authorized to obtain certain information under Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law No. 106-554, codified at 44 U.S.C. 3516, note) as well as TITLE 5 PART I CHAPTER 3 - 301, and 5 USC 552 - Sec. 552a

The Executive Order 9397 issued in 1943 allows Federal components to use the SSN exclusively whenever the component found it advisable to set up a new identification system for individuals, and requires the Social Security Board to cooperate with Federal uses of the number by issuing and verifying numbers for other Federal agencies.

The November 18, 2008 amendment to the Executive Order 9397 mandates Federal agencies to conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unlawful use.

Also see: 5 U.S.C. Chapter 552, 44 U.S.C. Chapters 21, 29, 31, and 33 (Records Management), and 18 U.S.C. 2071, 44 U.S.C. 3101 et seq., 44 U.S.C. 3506, Title 7 CFR 2.37, 36 CFR Chapter 12, Subchapter B, 36 CFR Part 1234, eGovernment Act of 2002 (Pub. L. 107-347, 44 U.S.C. Ch. 36), OMB Circular A-130, NARA - Disposition of Federal Records: A Records Management Handbook, NARA General Records Schedules.

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 personally identifiable information (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. Although the complete SSN displays onscreen, the SSNs are not shown on final reports. SSNs are redacted or truncated in reporting.

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 email, there are controls in place to ensure that 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:

FSIS Employee System - Data is downloaded from NFC on a weekly basis. The data is used for various FPC research tasks for validation purposes (create labels, reports, etc.).

NFC Pay Data System - The NFC Pay Data System is used to download pay 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.

Smead Imaging (TA/5110) - Used to maintain image files of all employee timesheets and billing documents. This system gives FPC Financial Technicians 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

FFIS Vendor Search System - Allows the Accounts Receivable Branch to research plant billing information and to provide labels for the 5110s for scanning/filing purposes. It is also linked to other database for validation purposes.

Any Audit reports that would contain PII are redacted and filtered as appropriate. The original reports never leave the FPC-GSS.

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.

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

The databases are used to ensure that payment, document requests, and audits reflect the appropriate individual. Requests can be made by FSIS investigators, LERD, and supervisors.

Without this type of access, employees with the same last name could have payments misapplied, incorrectly reported, or given misinformation. FPC-GSS utilizes the Access Database to validate employee information and provide reporting for individual FSIS employees. Reports include the following information: case reviews, disciplinary actions, OIG audits, agency variances, and employee record requests. In essence, more than one database is used to cross-correlate information and to ensure that the appropriate action is referring to the appropriate individual.

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 (up to 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.

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 FCP-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 USDA.

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 that personnel payroll records are processed properly, that employees and vendors are reimbursed for travel expenditures, and that USDA is reimbursed for services it provides.

If special requests come from Labor and Employee Relations Division (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 will not have PII information on them. If they do and the document is requested by LERD, Civil Rights, Courts, OIG, etc., any PII information is redacted from the image.

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. It is anticipated that FPC-GSS will be 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 with 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 Was notice provided to the individual prior to collection of information?

Yes. Notice is provided to FSIS employees at time of hiring, in accordance with Directive 8010.12, if personal information is obtained from an individual, he or she is provided with a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information.

6.2 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 in order to do business with FSIS.

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

No.

6.4 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?

Employees would work with Human Resources to ensure that the information is corrected. Information is available by default from payroll and other sources.

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

If personal information is incorrect, employees will likely be aware since payroll information will not be processed correctly. They can correct this information by contacting FSIS' Office of the Chief Human Resource Officer.

Individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700, Phone: (202) 690-3882, Fax (202) 690-3023, Email: fsis.foia@usda.gov.

The FOIA requestor must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her.

Non-employees would contact the technical services center within the office of policy and program development.

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

New employees are provided with such information at the time they are hired.

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 is 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 that 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 refresher training in order 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 email, there are controls in place to ensure that 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. Also, there is 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 18-May-2010.

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.

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 email, there are controls in place to ensure that 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 Application.

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"?

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

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.

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.

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- These technologies are not being used.

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

Cara LeConte –Director, FMD
Office of Chief Financial Officer
Food Safety and Inspection Service
United States Department of Agriculture

Alicemary Leach – Director, ECIMS
Office of Public Affairs and Consumer Education
Food Safety and Inspection Service
United States Department of Agriculture

Elamin Osman – Chief Information Security Officer
Office of the Chief Information Officer
Office of the Administrator
Food Safety and Inspection Service
United States Department of Agriculture

Janet Stevens - Chief Information Officer
Office of the Chief Information Officer
Office of the Administrator
Food Safety and Inspection Service
United States Department of Agriculture

PRIVACY IMPACT ASSESSMENT APPROVALS

Agreed: ______________________ 9/27/12
Cara LeConte Date
Director FMD/System Owner

Agreed: ______________________ 9-28-12
FOR Elamin Osman Date
Chief Information Security Officer (CISO)

Agreed: ______________________ 9/28/12
Janet Stevens Date
Chief Information Officer (CIO)

Agreed: ______________________ 9/27/12
for Alicemary Leach Date
Privacy Officer