Privacy Impact Analysis (PIA)

Financial Processing Center (FPC)

NFC Pay Data (PAYTA) Application

Revision: 2.2

Food Safety and Inspection Service (FSIS)

Date: January 2010

Document Information

Owner Details	
Name	Frederic Marks
Contact Number	301-344-0759
E-mail Address	Frederic.Marks@fsis.usda.gov

Revision History			
Revision	**Date**	**Author**	**Comments**
1.0	February 2008	Kevin O'Donovan for Dakota Consulting	Initial Version
1.1	May 2008	John Arrington	Quality Check
1.2	February 2009	Christopher Douglas	Converting to new '08 template
1.3	September 2009	Mikael Kebede	Quality Check
2.0	January 2010	Mikael Kebede	Converted to minor application specific PIA for the NFCPayData
2.1	January 2010	Mikael Kebede	Revised PIA based on comment from Privacy Officer
2.2	January 14, 2010	Olukayode Adeyosoye	Revised and updated PIA based on comments from Privacy Officer and formatted response section numbers.

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**
Janet Stevens	Chief Information Officer (CIO)	FSIS/OPEER/OCIO	202-205-9950
Ryan Cast	Chief Technology Officer (CTO)	FSIS/OPEER/OCIO/ OCTO	202-205-8285
Anthony Thompson	Assistant Administrator	FSIS/OM/OCFO	202-720-4425
Saurabh Baveja	Associated CIO (ACIO)	FSIS/OPEER/OCIO	202- 720-0294
Frederic Marks	Director, FMD	FSIS/OM/OCFO/FMD	301-344-0759
Michele Washington	C&A Functional Lead/Information System Security Officer (ISSO)	FSIS/OPEER/OCIO/ OCTO/ISSP	202-418-8832
Anita Holub	Chief, Accounts Receivable	FSIS/OM/OCFO/FMD	515-334-2024
Catherine Welles	Chief, Accounts Payable	FSIS/OM/OCFO/FMD	515-334-2002

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**
Doug Wike	IT Specialist Supervisor	FSIS/OPEER/OCIO/CSD	515- 334-2003
Elamin Osman	Information System Security Program Manager (ISSPM)	FSIS/OPEER/OCIO/OCTO/ISSP	202-720-5164
Mikael Kebede	ISSO Representative	FSIS/OPEER/OCIO/OCTO/ISSP	202-418-8934
John Nelson	FSIS Privacy Officer	FSIS/OPACE/ECIMS	202-720-2109

Table of Contents

1 System Information

System Information	
Agency:	Food Safety and Inspection Service
System Name:	Financial Processing Center (FPC) – NFCPayData Application
System Type:	☐ Major Application ☒ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Description of System:	The United States Department of Agriculture (USDA), Food Safety and Inspection Service (FSIS), Office of Management (OM), Chief Financial Officer (CFO), Financial Management Division (FMD), operates the Financial Processing Center (FPC), which is responsible for entry, verification, authorization, and processing of FSIS payroll and field payroll, travel and procurement payment documents representing approximately $500 million in salary payments, $20 million in travel reimbursements, and the annual collection of $100 million in revenues. The FPC was created in late 1996 as part of the reorganization of FSIS. As the FSIS national center for data processing and financial services, it supports approximately 9,500 – 10,000 permanent and 500 - 1500 Agency employees throughout the United States. Specifically, the FPC is responsible for the entry, verification, authorization, processing, and document management of field payroll, travel, billing, collections, debt management, and miscellaneous payments. The FPC provides financial information in various formats to the offices throughout the Agency and responds to inquiries and audits upon request. National Finance Center (NFC) Pay Data is one of the minor applications of the FPC GSS. This database was designed to house payroll data downloaded from NFC for purposes of reporting to many FSIS Program Areas.
Who owns this system? (Name, agency, contact information)	Frederic I. Marks Director, Financial Management Division Office of Management, Office of Chief Financial Officer Food Safety and Inspection Service, USDA 5601 Sunnyside Avenue, Room 2-1290 Beltsville, Md. 20705-5262 Office Phone: 301-344-0759 Frederic.Marks@fsis.usda.gov
Who is the security contact for this system? (Name, agency, contact information)	Doug Wike IT Specialist, (Team Leader) FSIS/OPEER/OCIO/CNSD/PCCSB 515-334-2003 Douglas.Wike@fsis.usda.gov
Who completed this document? (Name, agency, contact information)	Mikael Kebede 202-418-8934 Mikael.Kebede@fsis.usda.gov

2 Data Information

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	The Financial Processing Center (FPC) is responsible for the entry, verification, authorization, processing, and document management of payroll, travel, billing, collections, debt management, and miscellaneous payments. It supports approximately 9,500 permanent and 1000 temporary Agency employees throughout the United States. The FPC provides financial information in various formats to the offices throughout the Agency and responds to inquiries and audits upon request. National Finance Center (NFC) Pay Data is one of the minor applications of the FPC GSS. This database was designed to house payroll data downloaded from NFC for purposes of reporting to many FSIS Program Areas.
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	☒ Yes ☐ No – If NO, go to question 3. The data used includes a social security number collected from FSIS employee payroll data. FPC uses SSN as a unique identifier to be able to merge multiple tables into a desired report. The SSN will not be part of the final report that is sent to the various FSIS district offices and Headquarters.

No.	Question	Response
2.1	State the law or regulation that requires the collection of this information.	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. 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 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.

No.	Question	Response
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	☒ Yes ☐ No This system supports approximately 9,500 permanent and 1000 temporary Agency employees throughout the United States. The FPC provides financial information in various formats to the offices throughout the Agency and responds to inquiries and audits upon request. The use of SSN is necessary because it is a unique identifier available for FPC to be able to pull and merge various tables and produce reports.
4	Sources of the data in the system.	The source of the data is the FSIS employee payroll data (example, (the program) WebTA, PayPers and PayTA). The FPC inputs the data into pay system, and each record is authorized as they are input into the pay system. The FPC periodically pulls the data for validation and for report generation.
4.1	What data is being collected from the customer?	None
4.2	What USDA agencies are providing data for use in the system?	USDA's National Finance Center (NFC)
4.3	What state and local agencies are providing data for use in the system?	None
4.4	From what other third party sources is data being collected?	None
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	☐ Yes ☒ No – If NO, go to question 6.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	

2.2 Data Use

No.	Question	Response

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	This information is used for payroll and benefits management.
7	Will the data be used for any other purpose?	☐ Yes ☒ No – If NO, go to question 8.
7.1	What are the other purposes?	Not applicable
8	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists.)?	☐ Yes ☒ No – If NO, go to question 9.
8.1	Will the new data be placed in the individual's record (customer or employee)?	☐ Yes ☒ No
8.2	Can the system make determinations about customers or employees that would not be possible without the new data?	☐ Yes ☒ No
8.3	How will the new data be verified for relevance and accuracy?	Not applicable

No.	Question	Response
9	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	Information may be disclosed to an appropriate agency, whether Federal, State, or local, charged with the responsibility of investigating or prosecuting a violation of law, rule, or regulation, or order issued pursuant thereto, when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature and whether arising by general statute or particular program statute, or by rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative, or prosecutorial responsibility of the receiving entity. Information may be disclosed to the Department of Justice for the defense of suits against the United States or its officers, or for the institution of suits for the recovery of claims by the United States Department of Agriculture. Information may be disclosed to a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained. In such cases, however, the Member's right to a record is not greater than that of the individual. Records from this system of records may be disclosed to the National Archives and Records Administration and to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906 Information may be disclosed to agency contractors, experts, and consultants or volunteers who have been engaged by the agency to assist in the performance of a service related to this system of records and who need to have access to the records in order to perform the activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
10	Will the data be used for any other uses (routine or otherwise)?	☐ Yes ☒ No – If NO, go to question 11.
10.1	What are the other uses?	Not applicable

No.	Question	Response
11	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	☒ Yes ☐ No – If NO, go to question 12. Data is being consolidated from PayPers and payTA databases, not just one reporting system. The use of the SSN is necessary so that a unique identifier is used to merge data from multiple sources. For example, a typical report would detail how many employees in certain FSIS office have worked overtime or have taken sick leave in a certain time period.
11.1	What controls are in place to protect the data and prevent unauthorized access?	Windows Active Directory controls are used to prevent users from accessing information that they are not authorized to use. All users are required to undergo 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.
12	Are processes being consolidated?	☒ Yes ☐ No – If NO, go to question 13. This information is used for payroll and benefits management. The system is one of many minor applications of the FPC GSS, designed to house payroll data downloaded from NFC for purposes of reporting to many FSIS Program Areas.

No.	Question	Response
12.1	What controls are in place to protect the data and prevent unauthorized access?	All authorized staff using the system must comply with the Department'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. The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years. E-authentication is used to identify the Tracker user as authorized for access and as having a restricted set up responsibilities and capabilities with in the system. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory. By having a Department of Agriculture email account, their network login credentials are checked against authorized system user role membership and access privileges are restricted accordingly. FSIS system users must pass a government background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred. Annual, recurring security training is practiced and conducted through the Office of the Chief Information Officer. 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 of incomplete data as recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

2.3 Data Retention

No.	Question	Response
13	Is the data periodically purged from the system?	☒ Yes ☐ No – If NO, go to question 14. The data can go back 6 years. Any data more than 6 years old is purged according to guidelines provided by the National Archives and Records Administration (NARA).

No.	Question	Response
13.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	Data in paper and electronic format is maintained for a set period of time and then archived according to the National Archives and Records Administration (NARA) guidelines. These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). Backups are retained quarterly.
13.2	What are the procedures for purging the data at the end of the retention period?	Data is purged at the end of retention period in accordance with the Department's published records disposition schedules, based on the National Archives and Records Administration (NARA) Guidelines.
13.3	Where are these procedures documented?	The procedures are documented in the DR 3080-1 Records Disposition, which is the policies, responsibilities, and procedures for the orderly disposition of records within the Department of Agriculture. See http://www.ocio.usda.gov/records/policy.html DR 3080-1 Records Disposition
14	While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timely, and completeness to ensure fairness in making decisions. The controls include access control (Data is read only) and validation visually and based on pay period.
15	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	☒ Yes ☐ No SSN is necessary as unique identifier to be able to merge various data sources and to validate input. No other unique identifiers are stored in order to minimize the use of identifiers in accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501

2.4 Data Sharing

No.	Question	Response
16	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	☐ Yes ☒ No – If NO, go to question 17.

No.	Question	Response
16.1	How will the data be used by the other agency?	Not applicable
16.2	Who is responsible for assuring the other agency properly uses the data?	Not applicable
17	Is the data transmitted to another agency or an independent site?	☐ Yes ☒ No – If NO, go to question 18.
17.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	Not applicable
18	Is the system operated in more than one site?	☐ Yes ☒ No – If NO, go to question 19.
18.1	How will consistent use of the system and data be maintained in all sites?	Not applicable

2.5 Data Access

No.	Question	Response
19	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	FPC employees and administrators.
20	How will user access to the data be determined?	Users are the employees of the FPC. The users are responsible for different phases of financial processing for FSIS. Access to information is based on the role of the user. 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.

No.	Question	Response
20.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☒ Yes ☐ No The criteria, procedures, controls, and responsibilities are documented in the SSP as part of 2010 C&A package. 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. For example, Accounts Payable group and Accounts Receivable group have different access roles based on their job functions.
21	How will user access to the data be restricted?	Windows Active Directory controls are used to prevent users from access information that they are not authorized to use. Based on roles through the USDA e-Authentication program. USDA eAuthentication accounts allow users to do business with the government online. They provide access to authenticated sites (those that require passwords) that track contracts, programs, and services that involve users as a customer or technical service provider
21.1	Are procedures in place to detect or deter browsing or unauthorized user access?	☒ Yes ☐ No Information is only released on a 'need-to-know' basis under a statutory or other lawful authority to maintain such information. The information is used in accordance with the statutory authority and purpose. USDA agencies and offices will review the quality (including objectivity, utility, and integrity) of information before it is disseminated to ensure that it complies with the standards set forth in the Department's general information quality guidelines. FPC supervises user activities regarding the use and application of information system access controls, and utilizes automated controls and mechanisms, which support and facilitate the review of user activities. The FPC minor applications enforce separation of duties through distinct user roles and groups that the users are assigned. For system administrators, FPC ensure that individuals who are responsible for security do not also administer access controls or audit security logs, etc

No.	Question	Response
22	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	☒ Yes ☐ No If shared within FSIS and the Department of Agriculture, all information is still used in accordance with the system's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. All employees of the Department of Agriculture have undergone a thorough background investigation. 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 employees need to send data to NFC via email, there are controls in place to ensure that the data is encrypted.

2.6 Customer Protection

No.	Question	Response
23	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	The system owner will be responsible for protecting the privacy rights of all individuals whose data resides on this system. The System Owner is: Frederic I. Marks Director, Financial Management Division Office of Management, Office of Chief Financial Officer Food Safety and Inspection Service, USDA

No.	Question	Response
24	How can customers and employees contact the office or person responsible for protecting their privacy rights?	The system owner will be responsible for protecting the privacy rights of all individuals whose data resides on this system. FSIS Employees may request information from this system by contacting the system owner: Frederic Marks Director, Financial Management Division Office of Management, Office of Chief Financial Officer Food Safety and Inspection Service, USDA 5601 Sunnyside Avenue, Room 2-1290 Beltsville, Md. 20705-5262 301-344-0759 Frederic.Marks@usda.gov 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.
25	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	☒ Yes – If YES, go to question 26. ☐ No The USDA Breach Incident Response Policy (http://www.ocio.usda.gov/directives/doc/DM3505-000.htm) covers notification for this system.
25.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	Not Applicable
26	Consider the following: • Consolidation and linkage of files and systems • Derivation of data • Accelerated information processing and decision making • Use of new technologies Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	☒ Yes ☐ No – If NO, go to question 27. Yes. Multiple tables are merged so that various types of reports are produced.
26.1	Explain how this will be mitigated?	Not applicable

No.	Question	Response
27	How will the system and its use ensure equitable treatment of customers?	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.
28	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	☐ Yes ☒ No – If NO, go to question 29
28.1	Explain	Not applicable

3 System of Record

No.	Question	Response
29	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	☒ Yes ☐ No – If NO, go to question 30 The use of SSN is necessary because it is a unique identifier available for FPC to be able to pull and merge various tables and produce reports.
29.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	The data is retrieved by personal identifiers so that each individual is unique. SSNs are used to retrieve data, as are names.
29.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov.)	Not applicable
29.3	If the system is being modified, will the SOR require amendment or revision?	☒ Yes ☐ No WAIS Document Retrieval From the Privacy Act Online via GPO Access [wais.access.gpo.gov] [DOCID:agri_003-16] USDA/OP-1 - The location will be the only modification to the notification.

4 Technology

No.	Question	Response
30	Is the system using technologies in ways not previously employed by the agency (e.g., Caller-ID)?	☐ Yes ☒ No – If NO, the questionnaire is complete.
30.1	How does the use of this technology affect customer privacy?	Not applicable

5 Completion Instructions

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE FOR CYBER SECURITY.

Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Financial Processing Center General Support System

(System Name)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

Frederic Marks
System Owner

1/27/10
Date

Agency's Chief FOIA officer
OR Senior Official for Privacy
OR Designated privacy person

Date

Janet Stevens
FSIS OCIO

1/27/10
Date