Privacy Impact Assessment

Public Health Human Resources System (PHHRS)

- Version: 1.5
- Date: June 27,2012
- Prepared for: Food Safety and Inspection Service (FSIS), Office of the Chief Human Resources Officer (OCHRO)

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	May 2009	Dan Hill, SRA International, Inc	D R A F T
1.1	June 2009	Dan Hill, SRA International, Inc	Incorporated FSIS comments for v1.0
1.2	July 16, 2009	Dan Hill, SRA International, Inc	Incorporated Phase 2: Certification review comments for v1.1
1.3	August 5, 2009	Dan Hill, SRA International, Inc	Incorporated comments received from the Department and the Agency's Chief FOIA Officer for v1.2
1.4	November 10, 2009	Christopher Douglas	Incorporated the CTO comments.
1.5	June 27, 2012	Mark Whitaker	Updated to reflect new department template (from August 2010). Also, addressed comments from Phase 2 Concurrency review by the Department. Updated System Owner information.

Abstract

This document serves as the Privacy Impact Assessment for the PHHRS. The purpose of the system is to facilitate the employee performance review process for employees under the Public Health Human Resources System demonstration project. This assessment is being done in accordance with the Privacy Threshold Analysis conducted in March 2012.

Overview

The Public Health Human Resources System (PHHRS) is a new human resources pay-for-performance system for non-bargaining unit employees at FSIS that is changing the way employees are compensated, recognized, and rewarded. PHHRS manages two distinct programs – P3S and PACS. In addition, the OOEET Training Evaluation Tool falls under the PHHRS umbrella as a minor application.

P3S is the first system to be implemented in the PHHRS. P3S is the single, integrated source for performance rating and payout data for employees who have been converted to PHHRS. The purpose of the P3S application is to increase the efficiency of the pay pool process and help eliminate the potential for error when calculating employee pay increases. This is a web-based system, which automates tasks associated with performance management and pay pool processes. P3S is used to support the development of annual performance evaluations, ratings, and pay adjustments for FSIS employees.

The purpose of PACS is to empower supervisors within the FSIS operating units to create, classify, and generate unofficial position descriptions for all positions that are no longer being classified under the traditional General Schedule system. Higher levels of authority within the program business area will provide approval for these re-classified unofficial position descriptions. Authorized personnel within the FSIS Human Resources (HR) Office will have the final approval authority to make the unofficial position description an official description.

The purpose of the OOEET Training Evaluation Tool is to assess the effectiveness of training programs for inspection personnel and frontline supervisors, to assess the effectiveness of leadership development programs, and to assess training needs for FSIS employees. The tool allows FSIS to run reports based on the various evaluation survey data.

Processing Flow

P3S Process Flow

Below is a diagram that depicts the process flow from within the P3S application and its interfaces with other systems.

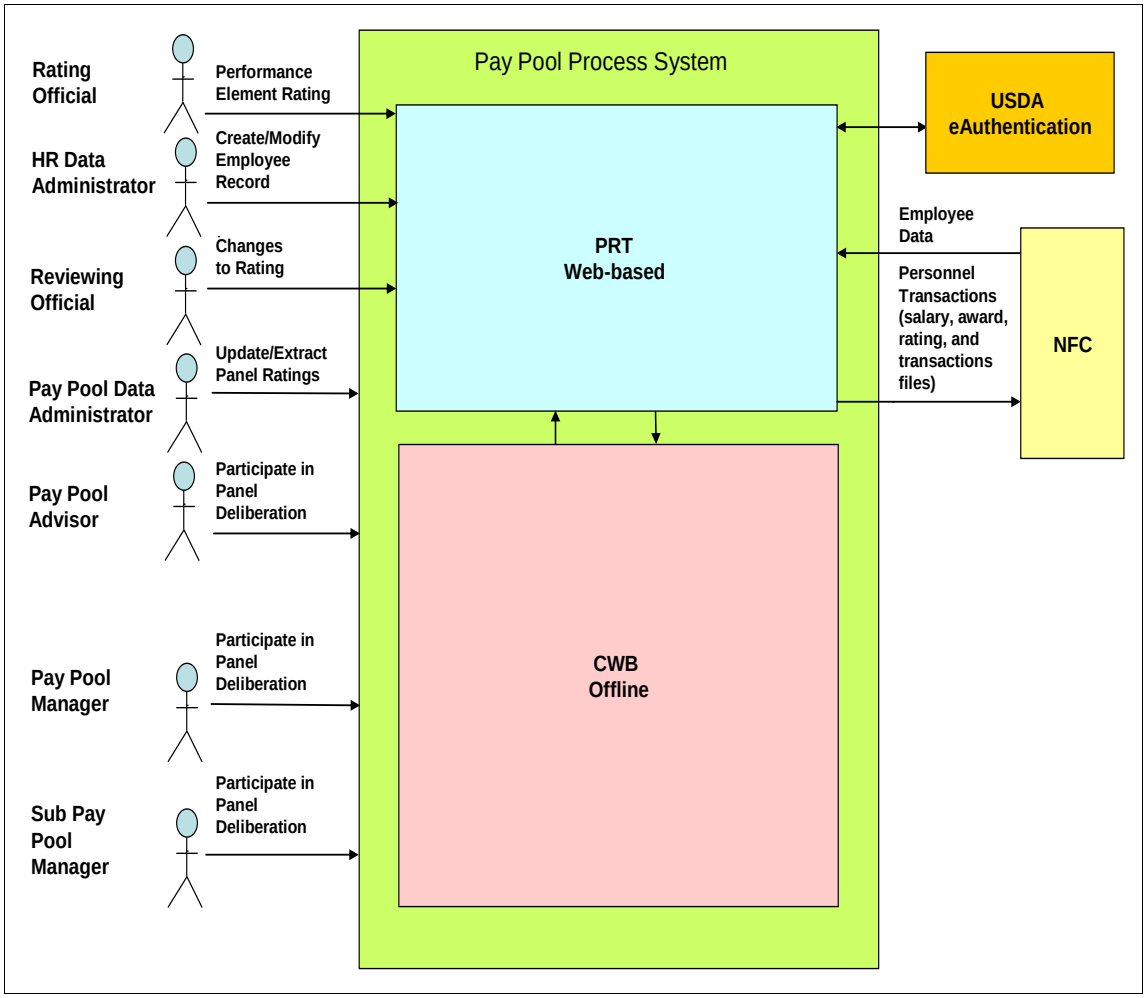

Figure 1: Process Diagram for the P3S Application

The P3S application has two components. The first component is the Performance Rating Tool (PRT), a database and Web-based application supporting the performance assessment process. It resides on a Web server and includes an SQL database. PRT is integrated with the existing information technology (IT) architecture, including USDA eAuthentication.

The second component is the offline Compensation Work Bench (CWB), an Excel-based application that supports the pay pool process. The CWB interfaces with the PRT for data transfers. The CWB user must initially log in to the PRT to be authenticated for an initial download of an Excel spreadsheet template and data. After the initial download and data import, the CWB Excel spreadsheet is able to run as a stand-alone system. When all pay adjustments have been made, the CWB user creates an export file, connects the workstation to the Intranet, logs into the PRT, and uploads the export file to the PRT database. Pay adjustments are made by the pay pool, so each Pay Pool Data Administrator has their own copy of the CWB template and data for their pay pool.

In terms of the P3S process flow from input to output, the following process takes place. The PRT is populated with employee and supervisor data. The data transfer is initiated by the USDA's National Finance Center (NFC) as a scheduled task and is completed via a file transfer protocol (FTP) server. The P3S receives USDA FSIS employee SSNs from the National Finance Center (NFC) that were originally provided to the NFC by USDA FSIS, along with other employee payroll data. P3S also transmits updated personnel and payroll information back to NFC's Payroll/Personnel System (PPS). A Virtual Private Network (VPN) is used for transmitting records to or from the NFC, so the information is encrypted during transmission.

PACS and the OOEET Training Evaluation Tool do not use SSNs.

The PRT supports performance raters as they complete performance assessments and determine new ratings. The PRT also supports the creation and maintenance of the FSIS pay pool structure. The PRT transfers rating data through the FSIS Intranet to the CWB.

The CWB imports a data file from the PRT to support pay pool deliberations, including the review of ratings and setting of pay increases and bonuses. When deliberations are complete and all updates to the CWB spreadsheet are entered, the Pay Pool Data Administrator creates an export file and transfers it to the PRT through the secure FTP server. The spreadsheet is also transferred as a completed record.

Once all the pay pools complete the process of reconciling ratings, salary increases, and bonuses, all of the final data resides in the PRT. Therefore, the PRT is the central source for rating and payout data.

Both systems are interactive and display, receive, and transfer payroll data. The CWB can compute statistics and generate employee payout reports. The PRT can also produce standard payout reports using data provided by the CWB, as well as other custom results using Business Objects.

The information being processed within the P3S application consists of employee performance evaluations, updated ratings, and updated base pay and bonus amounts. P3S does not use Social Security Numbers (SSNs) in its internal processing. SSNs are encrypted and stored only to maintain the association with a corresponding employee ID. The employee ID is used in place of SSNs for all P3S processing functions.

The USDA's eAuthentication system authenticates all user logins to the FSIS Intranet and to their authorized applications. SiteMinder works with eAuthentication to support user authentication to the application and to monitor session validity.

PACS Process Flow

Below is a diagram that depicts the PACS application process flow and how PACS interfaces with other systems. With the exception of the USDA eAuthentication service

(which is used for logging into PACS), the PACS application does not programmatically exchange information with other applications; instead, human intervention is required. An FSIS HR PACS user will manually update the NFC Position Management System Online (PMSO) system (a component of the NFC PPS) or manually update the employee's Electronic Official Personnel Folder (EOPF).

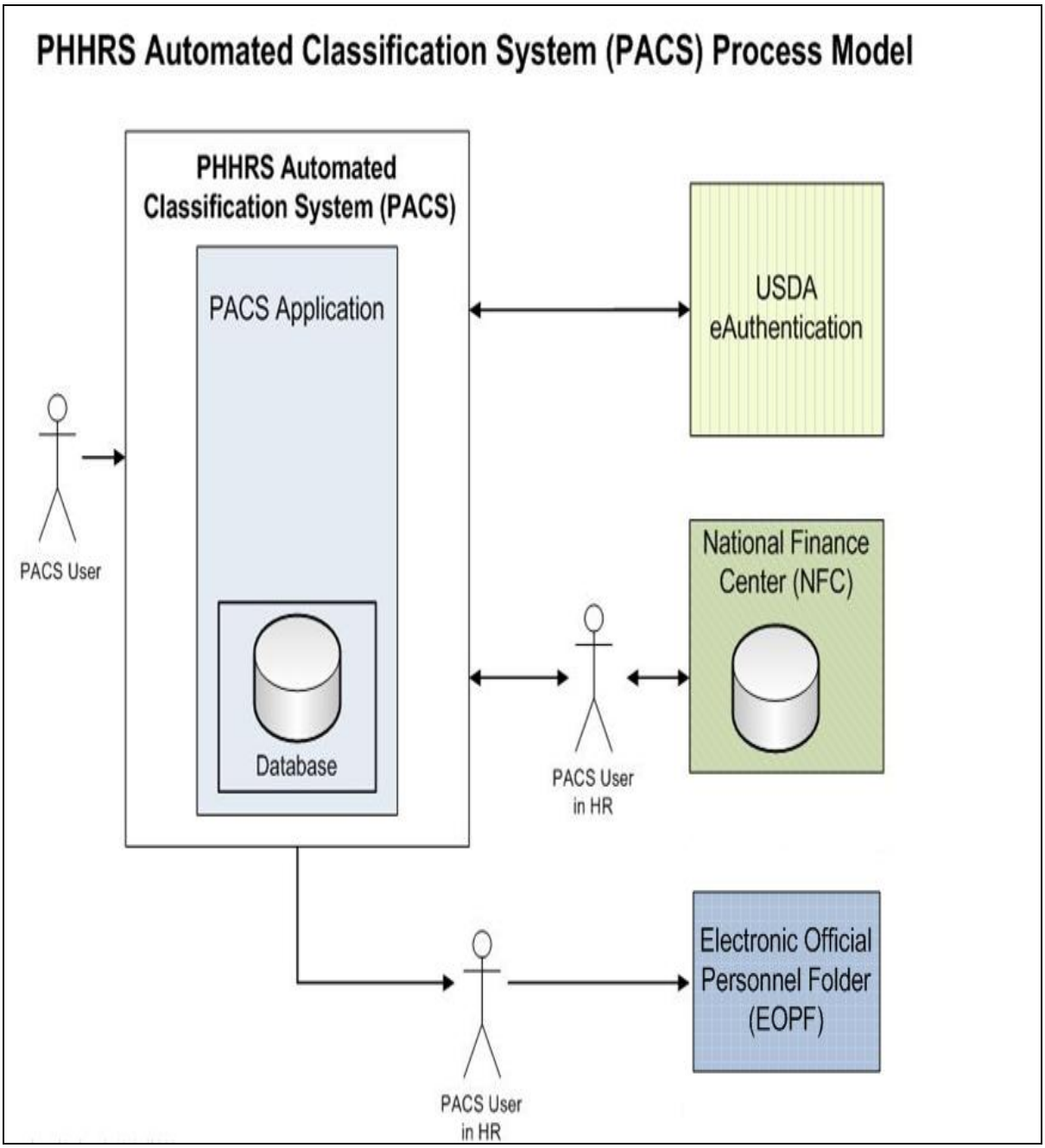

Figure 2: PACS Process Flow

The PACS component is used to develop FSIS Position Descriptions (PD). Within PACS, a PD can have an employee's name (however, a PD is not retrieved by a person's name). As the PACS Process Flow diagram shows, the FSIS HR team will manually update NFC (the PPS PMSO system) with new PD information; however, the PD ID # (also referred to as the Master Record #) is what is entered into the NFC system. With regard to the EOPF, the FSIS HR team will manually put a new PD into an employee's folder (which is their employment history).

OOEET Training Evaluation Tool Process Flow

Below is a diagram depicting the process flow from within the OOEET application and its interfaces with other systems.

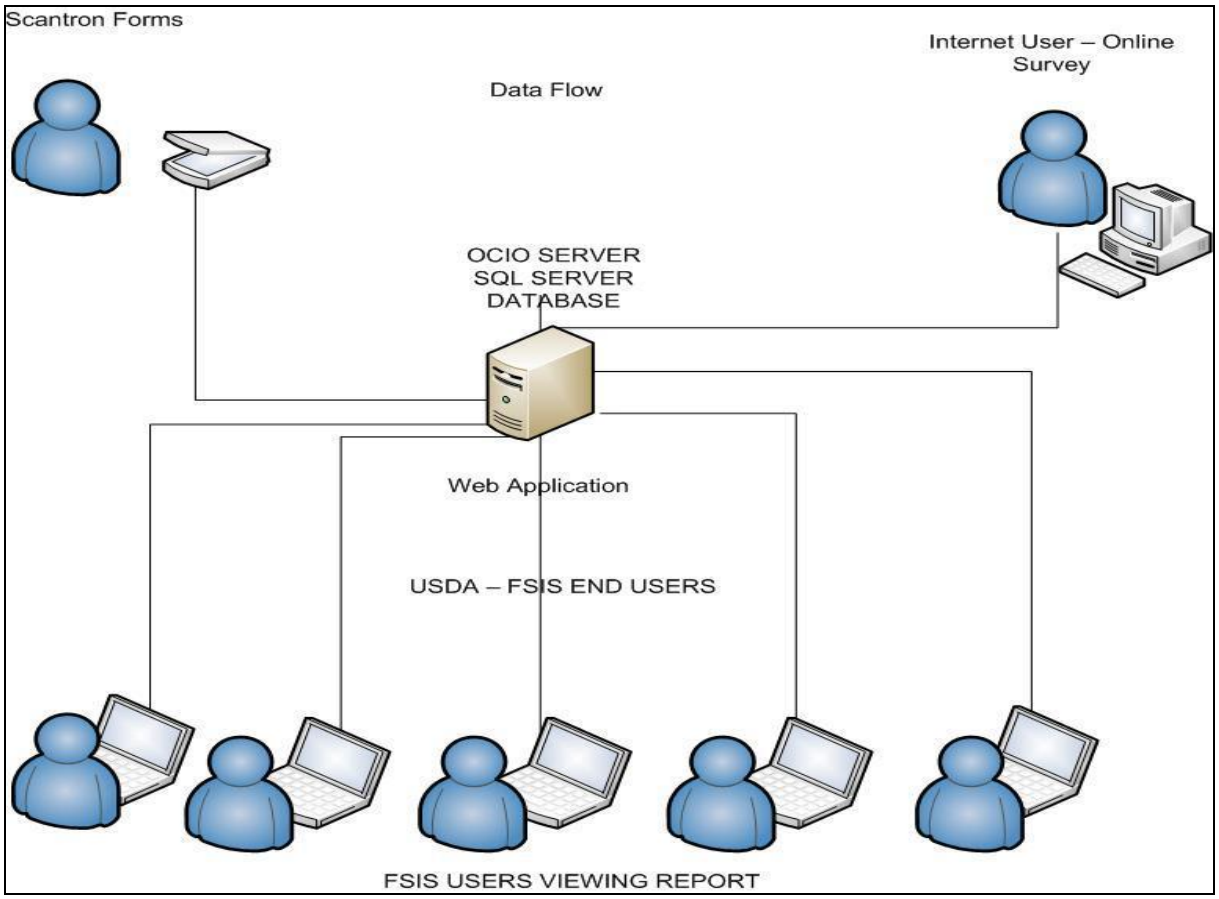

Figure 3: OOEET Training Evaluation Tool Process Flow

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.

FSIS will maintain the integrity of privacy-related information and comply with the statutory requirements to protect the information it gathers and disseminates. These include the Privacy

Act of 1974, as amended, the Paperwork Reduction Act of 1995, the Computer Security Act of 1987, the Freedom of Information Act, and OMB Circulars A-123, A-127, and A-130.

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 PHHRS system collects the following information for federal employees: First Name, Last Name, SSN, payroll data, Employment History (e.g., performance). NOTE: When a user is added to the P3S database, a unique number is associated with the user in the database. This number is indexed and used in the application for retrieving user records. This number is unique to PHHRS and is NOT the Employee ID that is used by HR.

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

The P3S component of PHHRS receives USDA FSIS employee SSNs from the NFC that were originally provided to the NFC by USDA FSIS, along with other employee payroll data.

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

The SSN is required by the NFC to process personnel action transactions. The NFC requires the personnel action transactions to be ready for updating the production database without additional data transformation on their part. Therefore, the full SSN is being retrieved in the automated interface to support the NFC requirement for including the SSN in the personnel action transactions.

Note: PHHRS receives the full SSN; however, it only saves and stores the last four digits of the SSN.

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 directs Federal agencies to conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unauthorized use.

1.4 How is the information collected?

The P3S component of PHHRS receives USDA FSIS employee SSNs via File Transfer Protocol (FTP) connection with NFC on a bi-weekly basis. The data is sent over a VPN, so the traffic is encrypted.

In addition, HR Administrators can manually add or modify an employee's record through the P3S user interface on an ad hoc basis.

1.5 How will the information be checked for accuracy?

The data is vetted at the time an employee is hired. The employee's information is conveyed to NFC for payroll purposes. So, when the information is provided back by NFC to FSIS for the PHHRS application the employee's information has already been vetted. In addition, the primary purpose for PHHRS is related to employ performance information. If an employee's information is incorrect, they will be able to ensure that it gets corrected.

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

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.

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 directs Federal agencies to conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unauthorized use.

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

The risk is that federal employee SSNs are collected and stored in the PHHRS system for an, approximately, bi-weekly matching process when updates are received from NFC. In addition, the employee name and employment history are also maintained. To mitigate the risks of using the SSN, the SSN is transferred from NFC to PHHRS via secure FTP (the traffic is encrypted). Additionally, 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. With regard to the employee and employment

history, the measures outlined below help mitigate the risk of maintaining this information. As such, this risk is a moderate risk.

PHHRS System Administrators and general users access the system using unique, authorized accounts. PHHRS cannot be accessed without an authorized account and it cannot be accessed by external users. There are no anonymous user accounts. All 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.

There are firewalls and other security precautions. 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. The security controls in the system are reviewed when significant modifications are made to the system, but at least every 3 years. Active Directory and PHHRS role-based security are used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system.

When anyone is granted access to the FSIS environment, they are issued a USDA email account and an FSIS user account (managed in Active Directory). In addition, they also have to obtain a USDA eAuthentication account to access PHHRS. To access PHHRS, the user must first login to the FSIS network environment by using their Active Directory account to login to their FSIS issued laptop. As a result, their secure network login credentials (from Active Directory) credentials are checked against authorized system user role membership, and access privileges are restricted accordingly. The USDA eAuthentication is used to login to PHHRS. When a user accesses PHHRS, there are PHHRS specific user roles that are used to further restrict a user's access. FSIS system users must pass a Government National Agency Check with Inquiries (NACI) background check prior to having system access. Regular, 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 or incomplete data as recorded in the system. Any contractors who may be authorized to access the system (e.g., 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 information (e.g., SSN) is used by PHHRS to ensure that employee data (e.g., performance rating) is associated with the correct person. The Employee Name and the ID assigned to the user by the application database can be used to retrieve employee information. Employee Name is not indexed in the application database. The ID is indexed in the application database.

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

PHHRS has a query function that allows records contained within the database to be retrieved based on one or more data elements (e.g. name). An analytic component built into the PHHRS platform allows the user (the employee or a supervisor) to review and edit (depending upon the user's role) employment history (e.g., performance reviews and ratings) records in the system.

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

PHHRS does not use commercially available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The risk is that federal employee SSNs are collected and stored in the PHHRS system. In addition, the employee name and employment history are also maintained. To mitigate the risks of using the SSN, the SSN is transferred from NFC to PHHRS via secure FTP (the traffic is encrypted). Additionally, 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. With regard to the employee and employment history, the measures outlined below help mitigate the risk of maintaining this information.

See Section 1.7 above for a description of the controls that have been put in place for PHHRS 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?

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). FSIS keeps accurate accounts of when and to whom it has disclosed personal records. This includes contact information for the person or agency that requested the personal records. These accounts are to be kept for 5 years, or the lifetime of the record, whichever is longer. Unless the records were shared for law enforcement purposes, the accounts of the disclosures should be available to the data subject upon request.

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 stored in the PHHRS system. To mitigate the risks of using the SSN, the SSN is transferred from NFC to PHHRS via secure FTP (the traffic is encrypted). Once the SSN is confirmed to be accurate for specified employee, the system stores only the last four (4) digits of each employee's SSN in PHHRS and the SSN fragment is encrypted when it is stored.

As long as employee SSN and employment data is retained, there is the risk that it may be disclosed to unauthorized individuals. To mitigate this risk, the system is maintained in an access-controlled facility and access-controlled network. In addition, logical access to the application and data is restricted to authorized personnel.

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

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within USDA.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

Per the PTA, PHHRS receives employee SSN from the USDA NFC, PHHRS transmits updated personnel and payroll information back to the USDA NFC via FTP on a secure VPN. In addition, the NFC Position Management System Online (PMSO) system (a component of the NFC PPS) is manually updated by HR personnel with information from PHHRS. PHHRS does not share information with other internal organizations.

4.2 How is the information transmitted or disclosed?

PHHRS (the P3S component) receives the employee SSN information over a USDA internal FTP connection with NFC. PHHRS also transmits updated personnel and payroll information back to NFC. The FTP connection is over a secure VPN. In addition, the NFC PMSO system is manually updated by FSIS HR personnel with information from PHHRS.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

The Microsoft .Net 3.5 AesManaged class (based on the AES encryption algorithm) is used to encrypt the FTP password. Once received, the SSN is hashed for processing. The last four digits are all that is stored in the PHHRS database. So, once received by PHHRS, employee SSNs are not maintained in the clear. The updated personnel and payroll information that is transmitted back to NFC is sent via FTP over a secure VPN connection.

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, the PHHRS 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 the National Archives and Records Administration (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, PHHRS does not share PII outside 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 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. In addition, PHHRS is covered by the 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 PHHRS information need to be shared with NARA, Congress, or the Department of Justice, standard FSIS guidelines for providing information to such organizations will be followed.

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

As long as employee SSN, name, and employment history data is transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee SSN, name, and employment history information 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. The data (name and SSN) is collected at the point of hiring.

In accordance with Directive 8010.12, if personal information is obtained from an individual, they are 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. In addition, PHHRS is covered by the SORN OP-1 (Personnel and Payroll System for USDA Employees).

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

Yes. However, the information is required in order to be hired and is covered by the SORN OP-1.

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

Covered under SORN OP-1.

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.

In accordance with Directive 8010.12, if personal information is obtained from an individual, they are 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. In addition, PHHRS is covered by the SORN OP-1 (Personnel and Payroll System for USDA Employees).

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?

The employee's SSN is important to the correct processing of an employee's information. If that is not correct, that will affect payroll and other functions. If an employee's pay or performance evaluations are not being processed correctly, they would work with Human Resources to ensure that the information is correct.

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

The employee would contact Human Resources (HR) and follow the standard HR procedures for addressing incorrect employee information.

In addition, users can contact the FSIS Service Desk at 1-(800) 473-9135.

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.

In addition, users can contact the FSIS Service Desk at 1-(800) 473-9135.

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

N/A- Formal redress is provided.

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

Corrections to the data are securely maintained in the same manner as the original data therefore, there is no privacy risk associated with redress available to individuals.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

To gain access to the PHHRS system, in addition to the standard FSIS user account used to login to FSIS issued laptops, PHHRS users must have a USDA eAuthentication user account and a role within the PHHRS application. The requirement for the USDA eAuthentication user account is addressed in PHHRS documentation along with the various PHHRS roles.

System Administrators and users of the system will have 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.

8.2 Will Department contractors have access to the system?

Yes.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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

Regular, recurring security training is practiced and conducted through the Office of the Chief Information Officer. Activity by authorized users is monitored, logged, and audited. All users are required to undergo Department-approved computer security awareness training prior to access and must complete computer security training yearly in order to retain access.

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

Yes, the ATO was granted on March 11, 2010.

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

Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database, following and implementing sound federal, state, local, department, and agency policies and procedures are safeguards implemented to mitigate the risks to any information technology.

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. Contractors authorized to access the system are governed by contracts identifying rules of behavior for USDA and FSIS systems and security. An access agreement describes prohibited activities (such as browsing). Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

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 primary risks are that the employee's information may be incorrect or that it may be disclosed to unauthorized individuals. These risks are mitigated by the following safeguards.

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

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?

PHHRS is a major application.
Reference the overview at the beginning of this document.

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"?

Both M-10-22 and M-10-23 have been reviewed by the 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.

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?

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

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

Robbie Terry – Acting Director, HR Demonstration Project Staff
Office of the Chief Human Resources Officer
United States Department of Agriculture

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

Elamin Osman – Chief Information Security Officer
Office of the Chief Information Officer
Office of the Administrator
United States Department of Agriculture

Janet Stevens – Chief Information Officer
Office of the Chief Information Officer
Office of the Administrator
United States Department of Agriculture

PRIVACY IMPACT ASSESSMENT APPROVALS

Agreed: _____ Date 6/27/12
Robbie Terry
System Owner

Agreed: Alicemary Leach Date 6-27-12
Alicemary Leach
Privacy Officer

Agreed: _____ Date 6-29-12
Elamin Osman
Chief Information Security Officer (CISO)

Agreed: _____ Date 6/29/12
Janet Stevens
Chief Information Officer