Privacy Impact Assessment

Human Resource Center GSS (HRC-GSS)

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.3	5/29/2012	Clinton A. Jackson	Updated the template design as well as included reference to the SF-52 minor application
1.4	8/13/2012	Clinton A. Jackson	Update to address PO comments.
1.5	9/27/2012	Noel A. Nazario	Update to address Theresa Cottery comments

Abstract

This Privacy Impact Assessment is being conducted because Human Resource Center GSS (HRC-GSS), as well as its SF-52 form (Request for Personnel Action) component, were identified during the Privacy Threshold Assessment as using PII. The HRC-GSS system provides human resources-related functions for the FSIS HRO (Human Resources Office). The SF-52 minor application, which is a part of the HRC-GSS system, allows users to submit SF-52 forms electronically.

Overview

HRC-GSS provides human resources-related functions for the FSIS HRO. The HRO is a sub-unit of the Human Resources Division (HRD) within the Office of Management (OM). The facility is housed in Minneapolis, Minnesota. The HRC-GSS consists of modules that help support the processing of HR-related forms and data. Three of the applications that are housed on the same server as HRC-GSS are separately owned and maintained by the Labor and Employee Relations Division. These three applications are:

- **Credit Card Delinquency**: This minor application pulls reports on employee usage of credit card (for travel) from the card issuing U.S. banks. The application produces delinquency letters that are mailed to the respective employee.
- **Employee Relations Log (ER Log)**: This minor application tracks the progress of employee disciplinary and adverse action cases, investigations, Hotline Complaints, etc.
- **Garnishment Log**: This minor application tracks open and closed cases relating to whether an employee's wages are applicable to being garnished. The application relies on records from the National Finance Center (NFC) to determine this status.

The HRC-GSS primarily consists of Access and MS SQL Server databases that support the mission of the HRD by allowing users to:

- Access portals to various HR data used by people both in and outside of the HR office within FSIS.
- Store information on people who donate leave to transfer recipients.
- Set up to track background investigations.
- Use an automated system to maintain requests for voluntary reassignments from bargaining unit employees who want to be reassigned to various locations and plants.
- Use an automated system to request vacancy announcements for Consumer Safety Inspector and Supervisory Consumer Safety Inspector positions.
- Log in a FedEx delivery received in the HRO.
- Request a service certificate for employees who have met the required years of service for a length-of-service certificate.
- Track employee folders to make sure they are sent to the administrative section and scanned in a timely manner.
- Log in all Equal Employment Opportunity complaint requests and notify the appropriate service team.

- Log information of employees who intend to travel and who need to fill a request for job-related expenses for approval. These items include:
    - travel expenses
    - materials for recruiting
    - flight information
    - credit card
    - time of departure and return
    - location where they are leaving from (office or residence location)
    - whether they are taking public transportation
    - requests for Internet access
    - type of event attending
    - request for flyers/promotion material
    - annual leave, comp time, work time, is requested, etc.
    - location destination
- Track and run reports on SF-52s.
- Track and monitor upcoming "suspense" actions, which are records entered by users to remind them of HR-related tasks that need to be performed by a date determined by said user. These include:
    - Student Loans: users are reminded when they are to receive payment as part of the recruitment scholarship program, which pays a participant specific sums yearly.
    - Generic recruitment incentives in which a user must process actions by a certain date to receive acknowledgement and benefits of their actions.
    - Referral bonus awards: Users, who have referred someone, will receive a reminder to process this referral after a year for a bonus.
    - Promotions: dated reminders of those who are in line for promotions.
- List employees who are eligible for priority consideration and eligible for re-promotion.
- Track awards and generate certificates.
- Store all-employee lists for use in various applications and reports.
- Calculate Service Computation dates.
- Store personnel actions for use in various applications and reports.
- Access the security suite, which contains each recommended security feature.
- Send out reminders for various HR items.
- Scan all files to track claims and worker compensation.
- Record all student internships/externships and applicants.
- Change APHIS agreement.
- Access a Reference for classifiers to look at each position in each program area.
- Send and receive OF5s (*Optional Form 5 – an inquiry as to availability form. Used to see if an applicant is still interested in a position*) to admin for letter printing.
- Track the departure and arrival of SACs (*Special Agreement Check – a form used in background investigations*) for processing.
- Track medical data to FOH (*Federal Occupational Health – usually used in the physical evaluation of potential or current employees).*

Processing Flow

The HRC-GSS application resides on the servers located in Minneapolis, Minnesota, and can only be updated by authorized HRO personnel.

For data input to occur into the HRC-GSS, an authorized user located in Minneapolis must input the data received from employees in hard-copy or electronic format. Data is also retrieved from the NFC and used to pull employee information to build an accurate profile. The servers have accounts set up for the remote users to connect to HRC-GSS via the USDA net work connection. Data is securely fed into each respective Minor Application on a daily basis. The system administrator at the Minneapolis location has control of the access levels into the HRC-GSS applications. The entire life-cycle (creating, managing, and revoking access) of access management is handled through Active Directory groups created within the HR Department.

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 to provide 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 types of information stored within HRC-GSS include USDA employee information, including name, home address, and job-related information, which includes position, grade, office location, awards, travel expenses, etc. The primary identifier for each individual whose information is stored in HRC-GSS is the HRID. HRID is used for processing and the field itself is displayed to some users, based on user authorization. This field can and is used for retrieval in lieu of using the social security numbers (SSNs).

The HRC-GSS administrator obtains reports from NFC and uses a script to import the employee data. The data in the NFC-generated reports include SSNs and are used to perform accuracy checks of FSIS employee data on HRC-GSS. Once the NFC report data are matched against the records on HRC-GSS, the SSNs are erased.

Establishment name and physical address, from PHIS, are also stored within HRC-GSS. PHIS reports in Excel format are imported in a manner similar to that of the data from NFC. The PHIS reports provide establishment data that is then used in lookup tables, reports, and drop down boxes in the HRC-GSS applications.

For the LERD-specific applications:

- Credit Card Delinquency: This minor application contains the employee's name, the term of the delinquency (30, 60, 90, 120 days, etc.), and the government credit card/account number that was used.

- Employee Relations Log: This minor application only maintains the employee's name.
- Garnishment Log: This minor application tracks open and closed cases as it relates to whether or not an employee's wages are applicable to being garnished. The application relies on records from the NFC to determine this status.

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

HRC-GSS uses data extracted from the NFC and the Public Health Information System (PHIS), input from HR personnel, and data entered by individual employees.

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

HRC-GSS information supports necessary HR functions related to employment, including hiring, leave, compensation, benefits, transfers, promotions, personnel actions, travel, administrative support, and workplace safety and fairness, among others. The LERD information supports other aspects of employment, including employee actions relating to discipline, investigations, complaints, wage garnishment, and employee delinquencies on government credit cards.

1.4 How is the information collected?

Reports generated on NFC and PHIS are imported through a manually activated script. Data is also entered by HR personnel or directly by individual employees. Employee input is collected via a web interface and populated in the user's user profile. Users must first have authorized access to the HRC-GSS application to update their data. Once approved, a user must be on the FSIS network, and log in with their specific HRID and password to reach their user profile.

Information from the NFC (see Section 1.2) is downloaded via Secure File Transfer Protocol. HRC-GSS runs a script against reports generated by the NFC and matches that data to its records to verify the accuracy of the employee data in the HRC-GSS. Reports generated on PHIS are downloaded as Excel files and then manually imported into HRC-GSS.

For the LERD-specific applications:

- Credit Card Delinquency: This minor application pulls reports on employee usage of credit card (for travel) from the card issuing U.S. banks. The employee's name is then cross-referenced with the HRC-GSS to identify the proper employee to receive the delinquency letter.
- Employee Relations Log: Only LERD administrators can submit data to the ER Database from where the ER Log pulls its information.

- Garnishment Log: Employee Relations specialists obtain employee's payroll information from NFC and enter it into the Garnishment Log application to determine if the employee is eligible for wages garnishment.

1.5 How will the information be checked for accuracy?

Information on HRC-GSS is matched every two weeks to data from NFC for accuracy. Employees have access to profile information that they can inspect for errors.

For the LERD-specific applications:

- Credit Card Delinquency: Employee names pulled from the card issuing banking institution are cross-referenced with the HRC-GSS employee name to ensure accuracy.
- Employee Relations Log: The application performs basic input checks, but LERD administrators are responsible for verifying the accuracy of the data they submit to the ER Database.
- Garnishment Log: Relies on NFC data to determine eligibility for wage garnishing. No checks are performed on the data, which is retrieved from NFC and is presumed accurate.

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

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 (44 U.S.C. 3101).

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

Access to data is strictly controlled, with access granted through HRSecure. HRSecure is an HRC-GSS-specific authentication process. Users must go through their specific program's security officer to place a request for access. From there, the user admin for HRSecure receives the request and establishes an account with the application.

HRC-GSS System Administrators and general users access the system using unique, authorized accounts. HRC-GSS 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 at the application level. 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 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. 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 HRSecure 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 e-mail account and an FSIS user account (managed in Active Directory). To access HRC-GSS, the user must first login to the FSIS network environment by using their Active Directory account to login. As a result, their secure network login credentials (from Active Directory) are checked against authorized system user role membership, and access privileges are restricted accordingly.

The USDA eAuthentication is not used to login to HRC-GSS, HRSecure is the native authentication system that is used. When a user accesses HRC-GSS, there are 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., software 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.

See the Overview and Section 1.3.

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

Data is accessed via web interface where users can log in to view their own HR information. Their primary means of logging in is via their unique HRID and their own password. Access queries can also be run on data, but the database is only accessible to the HRC-GSS administrator, who is granted access via his/her FSIS Active Directory permissions. HR personnel may generate reports that can be viewed online or in some applications exported to .pdf or .csv.

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

The system does not use any commercial or publicly available data.

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

In accessing the web interface for HRC-GSS, users have to go through an approval process through their own local security officer, and then the HRC-GSS administrator, to receive access to the system. Users also have to be in an applicable user group within the Active Directory, where the group is one that can warrant access for its members to the system. Once an account is created, a user must log in with their specific HRID and password. In order to access the application login interface the user must be on the FSIS network.

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?

Information is retained indefinitely. A record has yet to be deleted from the system.

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

According to the Records Management Office:
"The HRC-GSS is one of several electronic recordkeeping systems that are due to be scheduled over the course of this upcoming Fiscal Year. We have to report the completion of our electronic recordkeeping system schedules to NARA and the Department every year, and we are on track to have the majority of the systems scheduled ..."

The schedule can be accessed here:

https://inside.fsis.usda.gov/fsis/emp/static/global/offices/oSpace/asdOffice/informationBranch/recordsSection/recordsManagementOverview/recordsRDSchedules/rrdSchedules.jsp

If a user cannot access the schedule, they can contact the Records Management Office.

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

There are no additional risks associated with the length of time data is retained. Possible risks associated with the system data include unauthorized access to the users' profile, unauthorized users modifying a valid user's profile, and non-privileged users accessing database queries from the HRC-GSS. These issues are mitigated by measures listed in Section 1.7.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

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

All data is used by FSIS employees who have been approved to use the system and is not shared with external organizations. Regular employees only have access to their own profile information and employees with HR responsibilities have the ability to modify information on the users they are responsible for and to run HR reports where applicable.

4.2 How is the information transmitted or disclosed?

See Section 2.2.

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 controls, as noted in Section 1.7, mitigate the risk of internal sharing. The additional risk that a user might share personal data with someone who does not have authority to have that information is further mitigated by the fact that HR application users are routinely provided privacy reminders and take part in annual security awareness training. In addition, they are trained to handle sensitive and confidential information. All user data is only accessible and used by FSIS personnel who are authorized by their local security officer, and then by the HRG-GSS admin.

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?

Information may be shared in response to specific congressional requests, FOIA requests or, in rare cases, external entities. In these cases, personally identifiable information would be redacted.

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.

Generally, HRG-GSS application information is not shared with organizations external to the USDA. None of the LERD-specific applications (Garn Log, CC Delinq, and ER Log) partake in any external information sharing.

HRG-GSS is covered under Department SORN OP-1 (Personnel and Payroll System for USDA Employees).

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.

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

Should HRC-GSS application information need to be shared with NARA, Congress, or the Department of Justice, standard Departmental and 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 name, and employment history or other PII is transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

However, under normal operating circumstances, 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. Employee data, such as name and SSN are 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, HRC-GSS 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 as a condition of employment.

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.

As the employee provides the information, there is no risk that the individual is unaware of the collection. 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, the HRG-GSS application is covered by the SORN OP-1.

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 would contact HR and follow the standard HR procedures for addressing incorrect employee information. Keep in mind that much of the employee information is provided directly by the employee.

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

Individuals who believe that an HRG-GSS application might have inaccurate or erroneous PII 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) that gives the individual cause to believe that this system has records pertaining to him or to her.

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

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?

1) A user must be in a specific group/department that can justify use of the application. The network id/ip address ranges of user groups that can justify using the application are already defined. The HRC-GSS admin performs this task.

2) A justifiable user would then have to go to the new user request page for HRC-GSS and apply.

3) After the user submits the form, the security officer for that user's department must approve/decline the request. The officer is notified via e-mail.

4) Should the security office approve, the request is then sent to the HRC-GSS administrator.

5) Once approved, the user will have access to the system. The password that the user initially used to submit their request will become their main password to access the application.

8.2 Will Department contractors have access to the system?

Ordinarily no, however should a contractor be authorized to access the system, they will be governed by the contract's identifying rules of behavior for Department of Agriculture and FSIS systems and security. These types of contracts are routinely 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?

USDA Security Awareness and Privacy Training is provided to all users. As a condition of system access, users must successfully complete security training on a regular basis or lose system access rights.

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

Yes. The Certification & Accreditation was completed on 8/9/2010 and expires on 8/9/2013.

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

Audits are performed at both the hardware/OS level and at the application level. At the hardware level, the Engineering Branch uses Event tracker to monitor server logs, including user logins (failure and success), network connections, system processes, etc.

Audits on the application include:

- Bi weekly reports in which data from the NFC is compared to data within the application to ensure that an employee's overall federal information is accurate.

- Clicks and actions by the users are logged by the system.

The technical safeguards in place include regular vulnerability scans, which scan for vulnerabilities, irregular patch levels, and possible web application vulnerabilities. These scans are performed by the SOC (System Operation Center) and fixes are implemented by the engineering branch. Any security incidents that could possibly compromise the server or application are managed by the SOC Incident Response team.

8.6 <u>Privacy Impact Analysis</u>: 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 controls noted in Sections 1.7, 2.4, 3.3, and 4.3.

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?

HRC is a General Support System.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third-party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

No.

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

No 3rd party websites and/or applications are used.

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

No 3rd party websites and/or applications are used.

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

No 3rd party websites and/or applications are 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?

No 3rd party websites and/or applications are used.

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

No 3rd party websites and/or applications are used.

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

Not applicable as HRC-GSS does not use 3rd party applications.

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

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)?

No, it does not.

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?

No.

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.

HRC- GSS does not use 3rd party applications to access its data.

Responsible Officials

Jackie R. Shamblin – Director, OCHCO
Human Resources Division
Office of Management
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

Responsible Officials

Jackie R. Shamblin
FSIS/HRO
United States Department of Agriculture

PRIVACY IMPACT ASSESSMENT APPROVALS

Agreed: Jackie R Shamblin — 09/28/2012
Jackie R. Shamblin — Date
System Owner

Agreed: for Marvin Ryker — 9/28/12
Elamin Osman — Date
Chief Information Security Officer (CISO)

Agreed: Janet Stevens — 9/29/2012
Janet Stevens — Date
Chief Information Officer

Agreed: Alicemary Leach — 9/28/12
Alicemary Leach — Date
Privacy Officer