Privacy Impact Assessment

USDA Public Health Information System (PHIS)

- Version: 1.3
- Date: September 20th, 2012
- Prepared for: FSIS

United States Department of Agriculture

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.0	5/8/2012	DKW Communications, Inc.	Draft
1.1	7/12/2012	DKW Communications, Inc.	Revision per ISSP comments
1.2	7/16/2012	DKW Communications, Inc.	Revision per Comments from OPPD
1.3	8/19/2012	Najib Mirza (TistaTech Inc)	Revised to address common concern across and incorporate comments from SO

Privacy Impact Assessment for the Public Health Information System (PHIS)

July 19th, 2012

Contact:

Leonard Kenon
IT Project Manager
OA, OCIO-Enterprise Management Division
USDA Food Safety and Inspection Service (FSIS)
1400 Independence Ave., SW
Room 4905
Washington, DC 20250
(202) 690-3106

Reviewing Official:

Alicemary Leach
Privacy Officer (Acting)
Food Safety and Inspection Services
United States Department of Agriculture
(202) 690-3881

Abstract

This document serves as the Privacy Impact Assessment for the ***Public Health Information System (PHIS)****. The purpose of the system is to collect, consolidate and analyze data. This assessment is being done in conjunction with the PHIS Privacy Threshold Analysis.*

Overview

FSIS has developed the Public Health Information System (PHIS) as an effort to collect, consolidates, and analyze data. This public health based approach is in line with the core principles of the President's Food Safety Working Group. PHIS is a user-friendly, Web-based application that will replace existing applications, such as the Performance Based Inspection System (PBIS) and the Automated Import Information System (AIIS). The system is designed to integrate data from various agency systems and program areas for use as a tool in making the most informed decisions about inspections, sampling, policy, and other food safety activities to protect public health. It includes extensive information about domestic and foreign operations, product types, HACCP system, and so on. It creates a specific task for inspection personnel to periodically review and update establishment profiles. Authorized establishment personnel will be able to access and view their own profile in a future release. PHIS receives data from the Automated Commercial Environment (ACE) of the U.S. Customs and Border Protection (CBP). The customs broker or applicant submits entries into ACE. ACE then sends the data to PHIS, eliminating manual entry of importer's shipments into PHIS.

After obtaining a USDA e-Authentication (eAuth) account, authorized establishment personnel will be able to view certain data elements (limited to their establishment, generate a limited number of reports, and respond to and appeal noncompliance reports (NRs) in a future release.

PHIS enables FSIS personnel to document additional information for some procedures (e.g. "HACCP plan verified,""CCP and product involved," or "Lot number and specific regulations verified, as appropriate"). PHIS also stores Memorandums of Interview and notes for and on meetings with plant management. PHIS automatically generates follow-up tasks and adds them to task lists for inspection personnel to perform. This data will be available to authorized users in all FSIS program areas.

The diagram below depicts the end state major data flow between PHIS and various entities both internal and external.

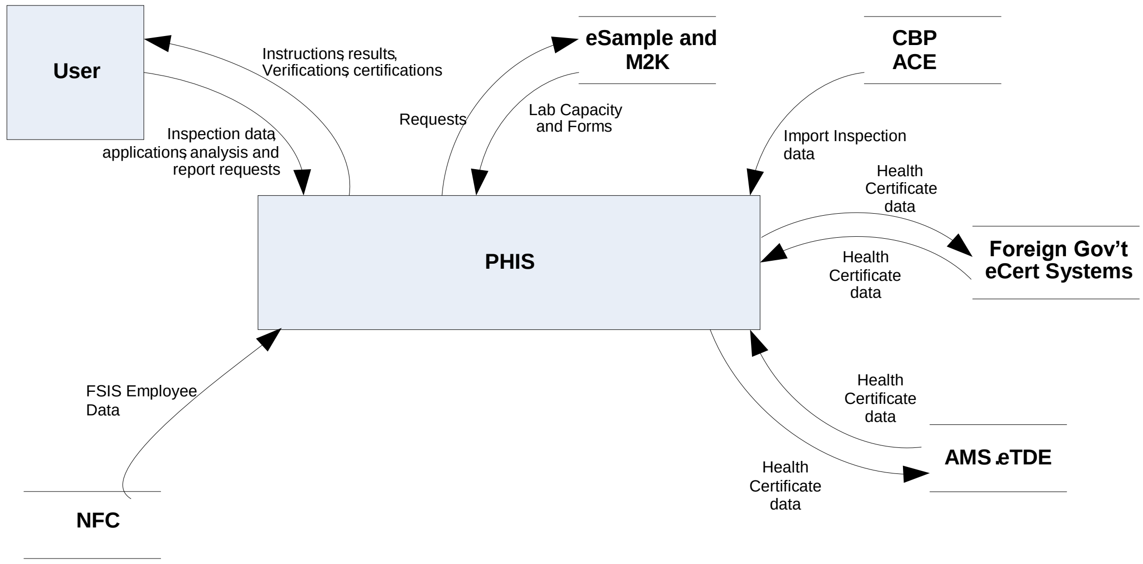

Figure -1 PHIS Conceptual Diagram

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 four modules within PHIS collect, use, disseminate or maintain the following information: Name (last name, first name of individual PHIS users or individuals conducting a transaction that is processed and/or stored within PHIS), establishment name, telephone number and address information (street or email address), personal identification number (e.g., tax identification number, agency assigned number, case number, permits, custom entry numbers etc.), and criminal history (if applicable) when registering for Grant Curator Role in PHIS.

The USDA National Finance Center (NFC) data feed includes complete employee roster data such as work schedule, position supervisory code, current employment status, etc.

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

Establishment data is provided to FSIS by designated establishment personnel, exporters, and importers. Data from other IT systems include the DHS/CBP ACE import application data, which is fed to PHIS for import inspection activity; user account information from the USDA eAuthentication system; and the Australian and New Zealand eCert data, which is also fed to PHIS for import inspection activity.

The specific FSIS agency employee data noted in section 1.1 above is obtained from the bi-weekly data feed from NFC.

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

The information is being collected to protect public health; to help enable informed decision-making about inspections, sampling, policy and other food safety activities; and to ensure the enforcement of the Federal Meat Inspection Act, the Poultry Products Inspection Act and the Egg Products Inspection Act.

1.4 How is the information collected?

Sources of this information are the official agency forms (on-line PHIS screens or actual paper form, when applicable) provided to the establishment or business entity acting on behalf of the establishment, legacy data previously provided by these entities and stored in FSIS application, and the comments made by FSIS reviewers of those forms. Additionally, data is also collected by inspection personnel receiving verbal input or reviewing establishment documents as part of their routine duties.

Data is provided to PHIS import modules through system interfaces such as DHS/CBP (ACE System), Australian and New Zealand eCert systems.

1.5 How will the information be checked for accuracy?

Inspection and district office personnel are required to update and maintain establishment profile data that is stored in PHIS, and establishment personnel have the ability and responsibility to review this information for accuracy. FSIS Office of Data Integration and Food Protection (ODIFP) also checks for the accuracy of information within PHIS. ODIFP is responsible for coordinating all of the Agency's data collection, analysis, and integration activities across program areas. ODIFP closely collaborates with other offices within FSIS to ensure adherence to emergency management policies, food defense directives, and the consistency and quality of data analyses.

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

The collection of information is regulated by the Federal Meat Inspection Act (FMIA), the Poultry Products Inspection Act (PPIA), and the Egg Products Inspection Act (EPIA).

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.

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

Privacy risks are minimized as addresses collected are business information and not personal. The information that is being collected includes individual names, establishment name and address. Access to data is strictly controlled, access is granted through the USDA-approved secure single sign-on application (eAuth – Level 2 Access), and authorization within PHIS is role-based to ensure least privileges.

PHIS cannot be accessed without an authorized account. PHIS System Administrators and general users access the system using unique, authorized accounts. This includes federal employees as well as users from industry and state meat and poultry inspection programs. 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. PHIS role-based security is used to identify the user as authorized for access and as having a restricted set of responsibilities and capabilities within the system.

The USDA eAuthentication process is used to login to PHIS. When a user accesses PHIS, there are PHIS specific user roles that are used to restrict a user's access. Also, 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.

PHIS integrates data from all agency systems and program areas for use as a tool in making the most informed decisions about inspections, sampling, policy and other food safety activities to protect public health.

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

Commercial reporting software tools, are used to design and generate reports for data analysis. PHIS has the capability to run internal, preprogrammed reports, such as trend reports and management controls for audit purposes, as well as ad hoc reports in response to specific events and congressional requests. These reports are created and maintained by the PHIS users and FSIS' Office of Data Integration and Food Protection, Data Analysis and Integration Group.

The predictive analytical module in PHIS uses predictive models and algorithms to analyze real-time data.

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

PHIS does not uses commercial (purchased or subscribed data from 3rd party sources) 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.

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 will be reviewed when significant modifications are made to the system, but at least every 3 years.*

In addition, privacy risks are minimized as information collected is predominantly business related. Access to data is strictly controlled, access is granted through the USDA approved secure single sign on application (eAuth – Level 2 Access) and authorization within PHIS is role based to ensure least privileges.

Authorized user login identifiers are appended to 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 recorded in the system. Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture and FSIS systems and security.

Controls are more completely described in section 1.7 above.

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?

Per 9 CFR 320, all PHIS records and data shall be retained for a specific retention period and then destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA). The data retention schedule described in DR 3080-001 Records Management outlines the procedures for archiving records.

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

Yes, the retention period has been approved by the FSIS records officer and the National Archives and Records Administration (NARA).

3.3 <u>Privacy Impact Analysis</u>: 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. PHIS enforces encrypted, controlled access based on eAuthentication, timeout for remote access, and system audit logs to ensure that information is handled in accordance with the above described uses. 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.*

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?

On a routine basis, information is shared with the USDA Inspection Personnel. PHIS also shares information with the M2K transactional database and the FSIS Data Warehouse. Information is written to the Data Warehouse from the PHIS transactional database to be used by other systems, The FSIS Data Warehouse provides a source of legacy system data and the analysis.

4.2 How is the information transmitted or disclosed?

USDA inspection personnel have direct access to PHIS after logging in via eAuthentication.

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.

Privacy risks are minimized as the information collected (establishment name and address, along with personal names) is predominantly business related. Access to data is strictly controlled, access is granted through the USDA approved secure single sign on application (eAuth – Level 2 Access) and authorization within PHIS is role based to ensure least privileges.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

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

PHIS information shared with organizations external to USDA includes foreign establishment export information and certifications for U.S. imports provided to *foreign governmental authorities, and access to outbreak information provided to personnel in the Department of Health and Human Services. In this specific scenario, information shared does not contain PII.*

In addition, lab samples, collected by domestic and import inspection personnel, are sent in some cases to non-FSIS labs. The results for sample collections are then returned to PHIS from the labs.

Specific PHIS reports (such as NR document) may include establishment or even FSIS inspection employee names that identify the establishment and location, or the establishment identifier (by which a work location could be determined). PII would be redacted if the information is being shared with other than the originating establishment.

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.

Yes, sharing of PII is compatible with the original collection as PII will be shared only with the entity that provided the original information. Data that is shared as part of a routine use is covered in a SORN under development. In the event that general data is shared with other than the original party (e.g., as part of noncompliance, in response to a FOIA, etc.) then the PII is redacted.

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

Information is shared either through direct access to and from PHIS or through hard copy reports. PHIS enforces encryption, controlled access based on eAuthentication, timeout for remote access and system audit logs to ensure that information is handled in accordance with the above described uses.

For the information sharing that occurs through hard copy reports or other means the safeguard are as follows –

PHIS inspectors can only generate and access reports related to their assignments and level of data access is strictly controlled through the implementation of least privileges when roles are assigned in PHIS. 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.

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

Privacy risks are minimized as the information that is being collected such as establishment name and address, along with individual names, is predominantly business related, and is ordinarily shared only with the establishment at which the information was collected or on that establishment's behalf (in the case of lab samples).

There are minimal privacy risks as PHIS enforces controlled access based on eAuth, authorization within PHIS is role based to ensure least privileges, timeout for remote access, data on is encrypted on the FSIS equipment such as laptops used by field personnel, and system audit logs to ensure that information is handled in accordance with the above described uses. Users are trained in the importance of data confidentiality.

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?

Notice is provided to FSIS employees prior to the collection of information. Neither industry nor state entities are required to provide similar notification.

Federal employees must complete an AD-1188 justification as part of the FSIS security clearance process before being granted access to USDA facilities and information systems. That notice contains the following information (note that PHIS does not contain SSN):

"The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information."

Contractors are required to complete a NACI (National Agency Check with Inquiries) prior to being granted access to USDA facilities and information systems. In the NACI, users are provided the following disclaimer in regards to their personal information:

"The information collected will be protected from disclosure under the Privacy Act of 1974. We do not retain or distribute collected information to any parties outside the

USDA, except as necessary to conduct official U.S. Government business, and we do not distribute this data to non-Government entities. Information collected will be retained at our discretion in a readable form for as long as necessary to complete the investigation. The information may be retained in an archival form as required by Federal laws and regulations governing the retention of historical records of Government agencies."

For non-FSIS-employees (primarily establishment employees), an earlier Notice of Request for a New Information Collection (Public Health Information System) was published in The Federal Register:
http://www.fsis.usda.gov/OPPDE/rdad/FRPubs/2010-0034.pdf

An official SORN will be available at a later date.

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

Federal employees have the opportunity and the right to decline to provide information, but the information (first and last name) is a requirement and condition of employment.

Similarly, the holder of the grant of inspection, often the establishment owner or chief operator, is afforded the opportunity and right to decline to provide information, but providing such information is a condition of the obtaining the grant. If the establishment owner/management chooses to use PHIS, it must provide the information needed to enroll and access PHIS. The employees at an establishment are covered by the privacy practices administered at that location. Regardless of the user type (internal or external), PHIS treats and safeguard all information with the same rigor.

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 notice is provided to inspection program personnel and contractors at the time of hiring, and to establishments when the plant applies for a grant of inspection, the risk of lack of awareness is limited to establishment employees who may not have been made aware by their employer that a small subset of employee names may be contained in the system (in noncompliance reports, etc.). As inspection program *personnel request names verbally on a regular basis, this risk is considered to be very limited.*

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

Individuals may submit a request to the FSIS Freedom of Information Act Office to request access to their information.

USDA employees may contact FSIS Human Resources (HR) to gain access to their PII information.

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

Any individual who has reason to believe that PHIS might have inaccurate or erroneous PII records pertaining to him or her 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.

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

New employees are provided with a Privacy Act Notice and an explanation of the notice at the time they are hired. Establishments are provided with a similar Privacy Act Notice and explanation at the time of the application for a grant of inspection.

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?

To gain access to the PHIS, users must have a USDA eAuthentication user account and a role within the PHIS application. The requirement for the USDA eAuthentication user account is addressed in PHIS documentation along with the various PHIS 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?

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 which has a privacy component is practiced and conducted through the Office of the Chief Information Officer. All internal users, including contractors, are required to undergo Department-approved Computer Security Awareness and Training (CSAT) prior to access and must complete CSAT yearly in order to retain access.

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

PHIS went through Certification and Accreditation (C&A) process and the ATO was granted on 2/16/2011 and it will expire on 2/16/2014.

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

PHIS enforces encryption, controls access based on eAuthentication, forces a timeout after a specified period of inactivity, and maintains system audit logs.

Authorized user login identifiers are appended to 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 recorded in the system. Certain PHIS tables have change data capture features turned on; this allows the database to retain old and new values along with who made the change and the time stamp.

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?

Privacy risks are minimized as primarily business name and address, along with limited individual names, are collected. All authorized staff using the system must comply with the Agency's general use policy for information technology known as "Rules of Behavior and Consequences". System use notifications are in accordance with the Privacy Act (subsection e[9]) and OMB Circular A-130, Appendix III.

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?

PHIS is a web-based major application for FSIS.

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

N/A

Section 10.0 Third Party Websites/Applications

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

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

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

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

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

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

N/A - Third party websites are not being used

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

N/A - Third party websites are not being used

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

N/A - Third party websites are not being used

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

N/A - Third party websites are not being used

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

N/A - Third party websites are not being used

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A - Third party websites are not being used

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A - Third party websites are not being used

10.10 Does the system use web measurement and customization technology?

N/A

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of 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

Leonard Kenon
OA, OCIO-Enterprise Management Division
Food Safety & Inspection Service
1400 Independence Ave., SW
Room 4905
Washington, DC 20250
202-690-2787

PRIVACY IMPACT ASSESSMENT APPROVALS

8/15/12

Scott Seebohm
System Owner
Date

9/19/12

Elamin Osman
Chief Information Security Officer (CISO)
FSIS/OPEER/OCIO/ISSP
United States Department of Agriculture
Date

Alicemary Leach
8-15-12

Alicemary Leach
Privacy Officer
Date

9/25/12

Janet Stevens
Chief Information Officer (CIO)
Food Safety and Inspection Services
United States Department of Agriculture
Date