USDA

Privacy Impact Assessment

AssuranceNet (AN)

Food Safety Inspection Service (FSIS)

Revision: 2.5

Date: December 02, 2009

Document Information

Owner Details	
Name	Jane Roth
Contact Number	202-720-8609
E-mail Address	Jane.Roth@fsis.usda.gov

Revision History			
Revision	Date	Author	Comments
2.2	6/11/2009	Tahir Rameez	Updated as part of C&A effort.
2.3	10/16/2009	Christopher Douglas	Updated document to address privacy office comments.
2.4	10/26/2009	Najib Baig	Updated document to address issues from Privacy Officer's questions/concerns. Old responses are retained for comparison and review purposes.
2.5	12/2/2009	Jeremy Wood	Updated points of contact and incorrect text.
2.6	12/10/2009	John Nelson	Grammar and other publicly presentation corrections. (Draft file located in the privacy office.)

Distribution List			
Name	Title	Agency/Office	Contact Information

Page ii

Date: November 03, 2009

This document contains Sensitive But Unclassified/Sensitive Security Information – Disseminate on a Need-To-Know Basis Only

1 System Information

System Information	
Agency:	Food Safety Inspection Service (FSIS)
System Name:	AssuranceNet
System Type:	☒ Major Application ☐ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low

Table of Contents

Description of System:	The FSIS is obligated to protect the public's health, which is susceptible to the effects of naturally occurring phenomena, of accidents, or of intentional acts that affect the food chain. FSIS must detect the threats as early and as specifically as possible so that it can mitigate them promptly.
	FSIS continues to strengthen its data communication and response infrastructure that protects public health as well as the integrity of the food and agricultural system. An early success to aggregate data across disparate systems has been the development of a data warehouse, which aggregates performance data from domestic and import inspection programs. The user interface for the data warehouse was accomplished through the development of the Enterprise Reporting System (ERS). The development of ERS has consolidated the existing reporting applications.
	AssuranceNet, a management control performance monitoring system, utilizes information from the data warehouse, as well, to monitor and alert management. AssuranceNet is a web-based application that transforms near real-time performance data into valuable decision-making information for managers. It currently extrapolates information from FSIS inspection and import databases plus employee responses to key questions in these areas, as well as administrative duties, to perform complex calculations that graphically display inspection performance indicators in a standard and traceable manner.
	IPPS (In-plant performance system) is a tool supervisors use to assess the performance of non-supervisory in-plant inspection program personnel. It focuses on ensuring that supervisors assess the work of inspection program personnel consistently and uniformly. In 2006, the Agency launched AssuranceNet. This system is used to capture IPPS assessment findings. Some of these findings feed into organizational performance measures in AssuranceNet for management control purposes. AssuranceNet is currently being expanded to monitor key management control performance measures for all FSIS program areas.
	The AssuranceNet Application Architecture provides the core application structure and common services for AssuranceNet. The structure consists of the components that provide the following services: • Application security • Application navigation • Business logic processing • Storage/retrieval of data to and from a database repository • Presentation of data • Creation and distribution of dynamic reports • Performance management • Document Management • Workflow Management
System Owner	Jane Roth Food Safety and Inspection Service 1400 Independence Avenue SW Washington, DC 20250 202-720-8609 Jane.Roth@fsis.usda.gov

Information System Program Manager	Jeremy Wood Food Safety and Inspection Service 901 D Street SW Washington, DC 20024 202-690-6298 jeremy.wood@fsis.usda.gov
Information System Security Program Manager (ISSPM)	Elamin Osman Food Safety and Inspection Service 1400 Independence Avenue SW Washington, DC 20250 202-720-4968 Elamin.Osman@fsis.usda.gov
C & A Functional Lead/Information System Security Officer (ISSO)	Michele Washington 1255 22nd St NW Washington, DC 20250 202-418-8832 Michele.Washington@fsis.usda.gov
Privacy Officer	John Nelson Food Safety and Inspection Service 1400 Independence Avenue SW Washington, DC 20250 202-720-4655 John.Nelson@fsis.usda.gov
ISSO Representative	Christopher Douglas 1255 22nd St NW Washington, DC 20250 202-418-8881 Christopher.Douglas@fsis.usda.gov

2 Data Information

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	Office of Field Operations and the Office of International Affairs use AssuranceNet to monitor their daily public health regulatory activities, and soon all remaining FSIS Program areas and functions will be incorporated into this system. The system monitors food safety and food defense management control performance measures. It is primarily used for compliance and enforcement data
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	☐ Yes ☒ No – If NO, go to question 3.
2.1	State the law or regulation that requires the collection of this information.	N/A
3	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.	☒ Yes ☐ No The system will improve the Agency's ability to schedule, analyze, and focus its resources on high-risk food safety and food defense in-commerce activities. It will provide all program offices with a central repository for reporting, managing and analyzing in-commerce data collected both within and outside of FSIS. This data will also be incorporated in the public health data infrastructure for analysis with other Agency data. The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.
4	Sources of the data in the system.	The sources of the information in the system are businesses and the information collected during visits and management controls. Information in the application comes from two general sources: • Data entered by FSIS employees as part of their inspection / surveillance / monitoring activities • Data retrieved from other backend FSIS applications primarily related to FSIS employee assignments and/or inspection data already collected
4.1	What data is being collected from the customer?	Strictly performance metric data.

No.	Question	Response
4.2	What USDA agencies are providing data for use in the system?	FSIS
4.3	What state and local agencies are providing data for use in the system?	None Though State and Local officials do provide input directly into the system (granted access), they are acting as contractors. The system does not receive from or send information to State and Local systems.
4.4	From what other third party sources is data being collected?	None
5	Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e., NFC, RD, etc.) or Non-USDA sources.	☒ Yes ☐ No – If NO, go to question 6. Data will be collected directly from FSIS customers during establishment visits and management controls.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	N/A
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	N/A

2.2 Data Use

No.	Question	Response
6	Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?	As part of the routine business process, individuals are informed in writing of the principal purpose of the information being collected from them. Data is collected for investigation and/or reporting purposes and to execute management controls.
7	Will the data be used for any other purpose?	☐ Yes ☒ No – If NO, go to question 8.
7.1	What are the other purposes?	N/A

No.	Question	Response
8	Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President	☒ Yes ☐ No The system will improve the Agency's ability to schedule, analyze, and focus its resources on high-risk food safety and food defense in-commerce activities. It will provide all program offices with a central repository for reporting, managing and analyzing in-commerce data collected both within and outside of FSIS. The data will also be incorporated in the public health data infrastructure for analysis with other Agency data. The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.
9	Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e., aggregating farm loans by zip codes in which only one farm exists.)?	☒ Yes ☐ No - If NO, go to question 10. The business process collects and extrapolates information from the FSIS inspection and imported databases plus employee responses to key questions in these areas, as well as administrative duties, to perform complex calculations that graphically display inspection performance indicators in a standard and traceable manner.
9.1	Will the new data be placed in the individual's record (customer or employee)?	☒ Yes ☐ No
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	☒ Yes ☐ No
9.3	How will the new data be verified for relevance and accuracy?	The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.

No.	Question	Response
10	Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?	As part of the routine business process, individuals are informed in writing of the principal purpose of the information being collected from them. Data is collected for investigation and/or reporting purposes and to execute management controls. Routine use for disclosure 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 or to the General Services Administration 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. USDA will disclose information about individuals from this system of records in accordance with the Federal Funding Accountability and Transparency Act of 2006 (Pub. L. No.109-282; codified at 31 U.S.C. 6101, et seq.); section 204 of the E-Government Act of 2002 (Pub. L. No.107 347; 44 U.S.C. 3501 note), and the Office of Federal Procurement Policy Act (41 U.S.C. 403 et seq.), or similar statutes requiring agencies to make available publicly information concerning Federal financial assistance, including grants, subgrants, loan awards, cooperative agreements and other financial assistance; and contracts, subcontracts, purchase orders, task orders, and delivery orders.
11	Will the data be used for any other uses (routine or otherwise)?	☐ Yes ☒ No – If NO, go to question 12.
11.1	What are the other uses?	N/A
12	Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?	☒ Yes ☐ No – If NO, go to question 13. This system is used to capture IPPS assessment findings. Some of these findings feed into organizational performance measures in AssuranceNet for management control purposes. AssuranceNet is currently being expanded to monitor key management control performance measures for all FSIS program areas.

No.	Question	Response
12.1	What controls are in place to protect the data and prevent unauthorized access?	All users are required to undergo computer security training prior to accessing the system and must complete refresher training in order to retain access. Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions. Multiple levels of access exist based on the authorized user's role and job function. The level of access for the user restricts the data that may be seen and the degree to which data may be modified by the user.
13	Are processes being consolidated?	☒ Yes ☐ No – If NO, go to question 14.

No.	Question	Response
13.1	What controls are in place to protect the data and prevent unauthorized access?	All authorized staff using the system must comply with the Department's general use policy for information technology. Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e [9]) and OMB Circular A-130, Appendix III.
		The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years. E-authentication is used to identify the Tracker user as authorized for access and as having a restricted set up responsibilities and capabilities with in the system. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory. By having a Department of Agriculture email account, their network login credentials are checked against authorized system user role membership and access privileges are restricted accordingly.
		FSIS system users must pass a government background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred. Annual, recurring security training is practiced and conducted through the Office of the Chief Information Officer.
		Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect of incomplete data as recorded in the system.
		Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of Agriculture systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	☐ Yes ☒ No – If NO, go to question 15.

No.	Question	Response
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	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).
14.2	What are the procedures for purging the data at the end of the retention period?	The procedures are documented in USDA's Records Management Policy, see 14.3.
14.3	Where are these procedures documented?	http://www.ocio.usda.gov/records/policy.html DR 3080-1 Records Disposition
15	While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timely, and completeness to ensure fairness in making decisions.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	☒ Yes ☐ No

2.4 Data Sharing

No.	Question	Response
17	Will other agencies share data or have access to data in this system (i.e., international, federal, state, local, other, etc.)?	☐ Yes ☒ No – If NO, go to question 18.
17.1	How will the data be used by the other agency?	N/A
17.2	Who is responsible for assuring the other agency properly uses the data?	N/A
18	Is the data transmitted to another agency or an independent site?	☐ Yes ☒ No – If NO, go to question 19.
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	N/A
19	Is the system operated in more than one site?	☒ Yes ☐ No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	The system is only operated at more than one site in the event of a contingency. The primary operations are at the NITC data center, whereas the alternate operations are at the USDA headquarters. In both cases, the system and its underlying data are protected via physical access control to the data center, as well as encrypted media.

2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	User, Administrator, Developer
21	How will user access to the data be determined?	There is a policy documented in the User Guide describing access permissions to the system. Additionally, there is a form that a potential user must complete for temporary access. Each program who has a module in the system determines user access to their module. 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.
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☒ Yes ☐ No The criteria, procedures, controls and responsibilities are documented in the User Guide. Each type of user has a specific type of User Guide, based upon the responsibility for that user.
22	How will user access to the data be restricted?	Based on roles through the USDA e-Authentication program. USDA eAuthentication accounts allow users to do business with the government online. They provide access to authenticated sites (those that require passwords) that track contracts, programs, and services that involve users as a customer or technical service provider.

No.	Question	Response
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	☒ Yes ☐ No Information is only released on a 'need-to-know' basis under a statutory or other lawful authority to maintain such information. The information is used in accordance with the statutory authority and purpose. USDA agencies and offices will review the quality (including objectivity, utility, and integrity) of information before it is disseminated to ensure that it complies with the standards set forth in the Department's general information quality guidelines.
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	☒ Yes ☐ No If shared within FSIS and the Department of Agriculture, all information is still used in accordance with the system's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. All employees of the Department of Agriculture have undergone a thorough background investigation. Access to facilities is typically controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

2.6 Customer Protection

No.	Question	Response
24	Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e., office, person, departmental position, etc.)?	The AssuranceNet Program Manager Jane Roth is responsible for protecting the privacy rights of individuals affected by the interface.

No.	Question	Response
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	The Program Manager's contact information is as follows: Jane Roth 1400 Independence Ave. SW, Room 3133-S Washington, DC 20250 Phone: 202-720-8609 Email: Jane.Roth@usda.gov. Technical service users can contact the USDA at 1-877-Pii2You or 1-888-926-2373, 24 hours a day, and then contact the FSIS Service Desk at 1-(800) 473-9135. Individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 1140, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 690-3882 Fax (202) 690-3023 - Email: fsis.foia@usda.gov. The FOIA requestor must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her.
26	A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?	☒ Yes – If YES, go to question 27. ☐ No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	N/A
27	Consider the following: • Consolidation and linkage of files and systems • Derivation of data • Accelerated information processing and decision making • Use of new technologies Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?	☐ Yes ☒ No – If NO, go to question 28.
27.1	Explain how this will be mitigated?	N/A

No.	Question	Response
28	How will the system and its use ensure equitable treatment of customers?	The system includes management controls and performance measures for supported activities that are reviewed by the supervisors, managers, and auditors to determine accuracy, relevance, timeliness, and completeness to ensure fairness in making decisions.
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	☐ Yes ☒ No – If NO, go to question 30
29.1	Explain	N/A

3 System of Record

No.	Question	Response
30	Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?	☒ Yes ☐ No – If NO, go to question 31
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	Some users are granted an access that allows for retrieval by name using a multi-tiered query.
30.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov.)	TBD
30.3	If the system is being modified, will the SOR require amendment or revision?	☐ Yes ☒ No

4 Technology

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

5 Completion Instructions

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

    1. Yes.

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

Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

AssuranceNet (AN)

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

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

_____   _____
System Manager/Owner   Date
OR Project Representative
OR Program/Office Head.

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

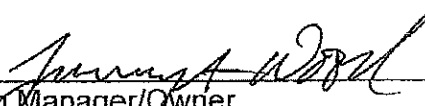_____   _____
Agency CIO   Date

Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

AssuranceNet (AN)

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

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

_____   12/4/2009
System Manager/Owner   Date
OR Project Representative
OR Program/Office Head.

_____   12/10/2009
Agency's Chief FOIA officer   Date
OR Senior Official for Privacy
OR Designated privacy person

_____   _____
Agency CIO   Date