Privacy Impact Assessment

USDA AssuranceNet (ANet)

- Version: 1.2
- Date: February 3rd, 2012
- Prepared for: FSIS

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

USDA AssuranceNet (ANet)

February 3, 2012

Contact Point

Vella Kay Holmes
Program Manager
Evaluation and Enforcement Division
Office of Program Evaluation, Enforcement and Review
Food Safety and Inspection Services
(202) 418-8817

Reviewing Official

Alicemary Leach
Privacy Officer (Acting)
United States Department of Agriculture
(202) 690-3881

Abstract

This document serves as the Privacy Impact Assessment for the USDA AssuranceNet (ANet). The purpose of the system is to monitor, analyze, and report the Agency's management controls effectiveness in meeting the agency's mission objectives. This assessment is being done in lieu of the Privacy Threshold Analysis conducted in February 2011.

Overview

The Food Safety and Inspection Service (FSIS) is the public health agency in the U.S. that ensures the nation's commercial supply of meat, poultry, and egg products are safe, wholesome, and correctly labeled and packaged. ANet supports the USDA FSIS in their efforts to monitor, analyze, and report the Agency's management controls. This centralized system allows supervisors and senior managers to obtain standard reports and create custom reports to monitor program areas' activities performance to ensure compliance with management controls and provide audit trails.

ANet is a web-based application that transforms near real-time (that is, data that is updated within 24 hours) performance data into valuable decision-making information for managers. It extrapolates information from various FSIS databases and allows for data entry to support specific management controls.

Presently, ANet supports Office of Field Operations (OFO), Office of International Affairs (OIA), Office of Policy & Program Development (OPPD), and Office of Program Evaluation, Enforcement & Review (OPEER) by defining management controls and calculating related performance measures.

A component of ANet is the In-Commerce System. The In-Commerce System is the Agency's compliance and enforcement system that supports OPEER, OFO, and OIA activities. The In-Commerce System includes the following compliance and enforcement activities: surveillance (food safety and food defense); product control (detention and seizure), investigation, and case management. Functionality includes reminders, the ability to print required forms, pre-populates forms, and the Stellent Document and Case Management System. Currently, the Stellent Document and Case management System supports OFO and OPEER by delineating the workflows that support specific enforcement activities through the In-Commerce System. In-Commerce will contain surveillance findings at firms and businesses that have previously violated the Federal Meat Inspection Act (FMIA), Egg Products Inspection Act (EPIA), and Poultry Products Inspection Act (PPIA), or that may be potential violators of these Acts, for which administrative, criminal or civil action may be taken.

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?

ANet has the Name(s) (last/first name) of designated person(s) representing the establishment/firm. It also has USDA/FSIS employee's name that uses ANet. Employee data comes from another system "RIS" which is component of Performance Based inspection system (PBIS).

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

Source of this information is Establishment or Business Entity.

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

Information is collected so that FSIS can enforce compliance with food safety related laws.

1.4 How is the information collected?

The information is collected by the district personnel (inspector) assigned to that establishment and compliance investigators who conduct surveillance and investigative activities at in-commerce businesses.

1.5 How will the information be checked for accuracy?

The data is verified by the inspector/investigator or their supervisor.

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

The legal mechanisms are under the aegis of Federal Meat Inspection Act, Egg Products Inspection Act and Poultry Products Inspection Act.

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

Privacy risks are very minimal due to the fact that name and addresses collected are strictly business information and not personal. Data collected is only for designated person representing the establishment plus this data is readily available and voluntarily give by the establishment.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

The data is used to conduct compliance and enforcement activities specifically: surveillance (food safety and food defense); product control (detention and seizure), investigation, and enforcement case management.

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

ANet is a web-based application that uses Crystal Reports and BusinessObjects Software Suite to transforms near real-time (that is, data that is updated within 24 hours) performance data into valuable decision-making information for managers. It extrapolates information from various FSIS databases and allows for data entry to support specific management controls. Thus it creates consolidated performance reports for FSIS Management.

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

N/A.

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.

ANet enforces controlled access based on eAuth, timeout for remote access and system audit logs to ensure that information is handled in accordance with the above described uses. In addition ANet is under an ATO and goes through Annual Self Assessment to comply with FISMA guidelines to ensure continuous security.

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?

As long as the information is valid (name of the designated person representing the establishment) it will be retained in the system.

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

Information is retained according to business rules of OFO, OIA, OPPD, and OPEER.

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

ANet enforces controlled access based on eAuth, timeout for remote access and system audit logs to ensure that information is handled in accordance with the above described uses. In addition ANet is under an ATO and goes through Annual Self Assessment to comply with FISMA guidelines to ensure continuous security.

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?

Information is shared based on the program area collecting data. ICS data is shared across OFO, OIA, and OPEER. Other data is contained within the program area (i.e. Equivalence is OIA only, Project Proposal is OPPD only).

4.2 How is the information transmitted or disclosed?

Other program areas have access to the data within the system. ANet enforces Controlled access, Timeout for remote access and System audit logs to ensure that information is handled in accordance with the above described uses.

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.

There is minimal risk associated with the data being shared internally.

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?

State inspectors and investigators have access to ANet as well. USDA/FSIS shares data based on request from the Congress.

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.

The legal mechanisms are under the aegis of Federal Meat Inspection Act and Poultry Products Inspection Act.

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

ANet enforces controlled access based on eAuth, timeout for remote access and system audit logs to ensure that information is handled in accordance with the above described uses. In addition ANet is under an ATO and goes through Annual Self Assessment to comply with FISMA guidelines to ensure continuous security.

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

There are minimal privacy risks as ANet enforces controlled access based on eAuth, timeout for remote access and system audit logs to ensure that information is handled in accordance with the above described uses. In addition ANet is under an ATO and goes through Annual Self Assessment to comply with FISMA guidelines to ensure continuous security.

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, for the ICS component of ANet, notice is provided in accordance with Directive 8010.2, Investigative Methodology by providing the individual a copy of FSIS Form 8000.5 Privacy Act Notice.

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

Yes, for the ICS component of ANet, if personal information is obtained from an individual, the individual is provided a copy of FSIS Form 8000.5 Privacy Act Notice, and an explanation of the Notice, prior to a request for the information and the individual may decline to provide the information.

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.

For the ICS component of ANet, in accordance with Directive 8010.2, if personal information is obtained from an individual, the individual is provided a copy of FSIS Form 8000.5 Privacy Act Notice and an explanation of the Notice prior to a request for the information.

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?

Non FSIS personnel cannot access ANet to view information. Individuals seeking notification of and access to any record contained in ANet, or seeking to contest its content, may submit a request in writing to the Headquarters or component's FOIA Officer, whose contact information can be found at http://www.da.usda.gov/foia.htm under "contacts.".

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

See 7.1 above.

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

Before providing information, the individual is presented with a Privacy Act Notice and an explanation of the Notice. The individual's acknowledgement of the Privacy Act Notice and the proffer of information signify the individual's consent to the use of the information. The purpose, use, and authority for collection of information are described in the Privacy Act Notice.

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

See 7.3 above.

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

Privacy risks are very minimal due to the fact that name and addresses collected are generally business information and not personal. Data collected is generally for designated person representing the establishment plus this data is voluntarily given by the establishment or individual.

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?

Access to ANet is strictly controlled and is based on business needs, user roles are well defined and access is tiered based. ANet require the user to enter a user name and password in order to gain access to the system. The department-wide eAuthentication process is used for AssuranceNet. Users must have level 2 authorization in order to access the system. Usernames and passwords are not stored within the AssuranceNet application. The application depends on eAuthentication to handle all authentication requests.

8.2 Will Department contractors have access to the system?

Yes, authorized departmental contractors will have access to the system

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.

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

Yes. The ATO was granted on 4/2/2010 and is scheduled to expire on 4/2/2013.

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

ANet enforces Controlled access, Timeout for remote access and System/database audit logs.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Privacy risks are very minimal due to the fact that name and addresses collected are strictly business information and not personal. Data collected is only for designated person representing the establishment plus this data is readily available and voluntarily give by the establishment.

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?

ANet 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 - Third party websites are not being used.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

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

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

Jane Roth

ANet System Owner

United States Department of Agriculture

Approval Signatures

Alicemary Leach
Privacy Officer (Acting)
United States Department of Agriculture

Jane Roth
System Owner (SO) - ANet
Food Safety and Inspection Services
United States Department of Agriculture

Elamin Osman
Chief Information Security Officer (CISO)
Food Safety and Inspection Services
United States Department of Agriculture

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

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
1.1	1/6/2010	Najib Mirza	Draft created after ANet ATO in 2009
1.2	2/3/2012	Najib Mirza	Fully signed (in 2011) and yearly (2012) reviewed PIA