Privacy Impact Assessment

AssuranceNet (AN)

- Version: 9.0
- Date: February 1, 2020
- Prepared for: FSIS

United States Department of Agriculture

Privacy Impact Assessment for the

AssuranceNet (AN)

February 1, 2020

Contact Point

Scott C. Safian
Office of Investigation, Enforcement & Audit
Phone: 202-418-8872
355 E St., SW, Washington, DC 20024

Reviewing Official

Privacy Office
United States Department of Agriculture

Revision History*

Document Revision and History			
Revision	**Date**	**Author**	**Comments**
4.0	01/07/2015	Marie Penninger	Annual Assessment Review
4.5	09/01/2015	Marie Penninger	Incorporate SO Comments
4.6	3/24/2016	Marie Penninger	Incorporate CISO Comments
4.7	3/24/2016	Marie Penninger	Incorporate Privacy Review Comments
5.0	03/21/2016	Marie Penninger	ATO Update
6.0	09/22/2016	Marie Penninger	Annual Assessment FY2017
6.5	09/01/2017	Marie Penninger	Annual Assessment FY2018
7.0	12/11/2017	Marie Penninger	Annual Assessment FY2018 Complete
7.1	08/31/2018	Marie Penninger	ATO Assessment FY2019
7.2	12/22/2018	Marie Penninger	Privacy Comments FY2019
8.0	03/21/2019	Marie Penninger	Signature Cycle Complete
9.0	02/01/2020	Marie Penninger	Annual Assessment FY2020

***NOTE:** *During Annual Assessment, the System Owner and/or Information System Security Officer (ISSO) Representative reviews this Privacy Impact Assessment (PIA). A Revision number is identified in the table to represent this annual review, although no document signatures are required unless significant system/organizational document changes are involved.*

Abstract

This document serves as the Privacy Impact Assessment (PIA) for the United States Department of Agriculture (USDA) AssuranceNet (AN). The purpose of the system is to collect, consolidate, and analyze detailed information regarding in-commerce facilities and provide decision making points that protect public health and enforce compliance with food safety related laws. This system is also used to collect, consolidate, and analyze detailed information related to employee misconduct investigations. This assessment is being done in conjunction with the AN Privacy Threshold Analysis conducted in September 2015 and reviewed annually.

Overview

The Food Safety and Inspection Service (FSIS) is the public health regulatory agency operating within the USDA. The Agency ensures the commercial supply of meat, poultry, and processed egg products prepared for distribution as human food is safe, wholesome, and accurately labeled. FSIS works diligently with our partners, including other federal, state, and local government agencies, industry partners, food handlers, and consumers to prevent foodborne illness and promote safety.

AN 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.

AN 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, AN supports Office of the Administrator (OA), Office of Field Operations (OFO), Office of Policy & Program Development (OPPD), and Office of Investigation, Enforcement and Audit (OIEA) by defining management controls and calculating related performance measures.

A component of AN is the In-Commerce System (ICS). ICS is the Agency's compliance and enforcement system that supports OIEA and OFO activities. ICS 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-populate forms, and the Stellent Document and Case Management System. Currently, the Stellent Document and Case management System supports OFO and OIEA by delineating the workflows that support specific enforcement activities through the In-Commerce System. Another component of AN is the

Misconduct Investigation Module. The functionality includes the ability to print required forms and pre-populated forms.

ICS 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 (PPA), or that may be potential violators of these Acts, for which administrative, criminal or civil action may be taken. The Misconduct Investigation Module will contain investigation findings for which administrative actions may be taken. The legal authority to operate AN is provided by the signed Authority to Operate (ATO) letter dated 03/28/2022.

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?

AN 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 AN. AN also maintains criminal history, miscellaneous identification numbers, and handwriting or signature images. The Misconduct Investigation Module also has the Name(s) of subjects and/or complainants as identified in complaints address information for businesses and sometimes business owners. Violation information and corporate structure information is also collected.

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

The sources of the information in the system are the Establishment, Business Entity or Individuals.

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

The information is being collected to protect public health and enforce compliance with food safety related laws and administrative actions.

1.4 How is the information collected?

The information is collected by the district personnel (inspector) assigned to that establishment and investigators who conduct surveillance and investigative activities as well as Misconduct Investigators.

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 November 18, 2008 amendment to the Executive Order 9397 mandates Federal agencies to conduct agency activities that involve personal identifiers in a manner consistent with protection of such identifiers against unlawful use.
44 U.S.C. 3101 states that 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.

7 U.S.C. 2204 states that the Secretary of Agriculture may conduct any survey or other information collection, and employ any sampling or other statistical methods, which the Secretary determines is appropriate. USDA is also authorized to obtain certain information under Section 515 of the Treasury and General Government Appropriations Act for Fiscal Year 2001 (Public Law No. 106-554, codified at 44 U.S.C. 3516, note), as well as 5 U.S.C. PART I, CHAPTER 3 - 301 and 5 U.S.C. 552 - Sec. 552a

Also see: 5 U.S.C. 552; 44 U.S.C. Chapters 21, 29, 31, and 33 (Records Management); and 18 U.S.C. 2071; 44 U.S.C. 3101 et seq.; 44 U.S.C. 3506; Title 7 CFR 2.37; 36 CFR Chapter 12, Subchapter B; 36 CFR Part 1234; eGovernment Act of 2002 (Pub. L. 107-347, 44 U.S.C. Ch. 36); OMB Circular A-130; NARA - *Disposition of Federal Records: A Records Management Handbook*; NARA General Records Schedules.

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

The information being collected includes individual names, establishment name and addresses. Privacy risks are minimized because 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 AN is role-based to ensure least privileges.

AN cannot be accessed without an authorized account. AN System Administrators and general users access the system using unique, authorized accounts. All users are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those 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.

AN utilizes firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for IT. 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. All of the security controls in the system are reviewed when significant modifications are made or at least every three years. The System Security Policy (SSP), and a subset of these controls, is also reviewed annually. AN 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 e-Authentication process is used to login to AN. When a user accesses AN, there are AN specific user roles that restrict access. Also, FSIS system users must pass a Government National Agency Check with Inquiries (NACI) background check prior to being granted system access. Regular, recurring security training is 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 recorded in the system. Any contractors who may be authorized to access the system, such as software developers, are governed by contracts identifying rules of behavior for USDA, FSIS systems, and security. Contracts are reviewed upon renewal by management and contract personnel experts.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The information 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. The information is also used as a centralized location to contain evidence for employee misconduct investigations.

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

AN is a web-based application that uses Crystal Reports and Business Objects Software Suite to transform near real-time performance data into valuable decisionmaking information for managers. It extrapolates information from various FSIS databases and allows for data entry to support specific management controls. 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.

AN does not use commercial (purchased or subscribed data feed 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.

AN utilizes firewalls and other security precautions. For example, all authorized staff using the system must comply with the Agency's general use policy for IT. 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. All of the security controls in the system are reviewed when significant modifications are made or at least every three years. The SSP and a subset of these controls are also reviewed annually.

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 (eAuthentication – Level 2 Access).

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 Code of Federal Regulations 320, all AN 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/NARA.

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

The length of time data is retained does not change the level or type of risk associated with data retention. AN enforces encrypted, controlled access based on eAuthentication, timeout for remote access, and system audit logs to ensure 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 IT. 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?

Information is shared based on the program area collecting data. AN and ICS data is shared across all FSIS program areas and other USDA entities on a need to know

basis. 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?

AN 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.

Access to data is strictly controlled and is granted through the USDA approved secure single sign on application (e-Auth – Level 2 Access).

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 AN data and USDA/FSIS shares data based on requests from Congress, and USDA entities to include OIG, OGC, and other USDA agencies.

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.

Sharing of PII is compatible with the original collection. AN is in the process of developing a SORN which is being tracked by POA&M 18823 – C&A FY2013 PL-5: SORN is Missing for ANet .

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

Should AN information need to be shared externally, departmental guidelines for providing information to such organizations will be followed. This includes the redacting of PII, unless the information is required under law.

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

As long as employee PII data is transmitted externally, there is the risk that it may be disclosed to unauthorized individuals.

Under normal operating circumstances, employee 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. Notice is provided to the FSIS employees at time of hiring, in accordance with Directive 8010.2 for all Source System users. Plant vendors are provided notification during business agreement processes. If personal information is obtained from an individual, he or she is 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.

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

Yes, individuals do have the opportunity and/or the right to decline information. 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. This does not apply to government employees.

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, individuals do not have the right to consent to particular uses of the information.

This does not apply to government employees.

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

In accordance with Directive 8010.2, 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?

Individuals who have reason to believe that this system might have records pertaining to them should write to the FSIS FOIA office.

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 2168, 1400 Independence Avenue, SW Washington, DC 20250-3700 - Phone: (202) 720-2109- Fax (202) 690-3023 – E-mail: fsis.foia@fsis.usda.gov.

For more information about how to make a FOIA request, please see:

http://www.fsis.usda.gov/wps/portal/footer/policies-and-links/freedom-of-informationact/foia-requests

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

Any individual who has reason to believe that AN might have inaccurate or erroneous PII records pertaining to him or her should contact the FSIS FOIA Officer. The FOIA requestor must specify 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, and 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?

Before providing information, the individual is presented with a Privacy Act Notice and an explanation of the Notice, on both the Form 7234-1 and Form 8822-4. 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?

N/A – Formal redress is provided.

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

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

Section 8.0 Technical Access and Security

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

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

Access to AN is strictly controlled and is based on business needs, user roles are well defined and access is tier based. AN requires 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 AN. Users must have level 2 authorization in order to access the system. Usernames and passwords are not stored within the AN 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?

Regular, recurring security training which has a privacy component is 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 prior to being granted access and annually thereafter to retain access.

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

AN went through the Security Assessment and Authorization (SA&A) process. The ATO was granted on 03/31/2016 and will expire on 03/31/2019.

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

AN enforces controlled access based on e-Authentication, forces a timeout after a specified period of inactivity, and maintains system 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 minimized as primarily only business names and addresses are collected. All authorized staff using the system must comply with the Agency's general use policy for IT 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?

AN 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.

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"?

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

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

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

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

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

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

N/A - Third party websites are not being used

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

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

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

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

If so, is it done automatically?

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

If so, is it done on a recurring basis?

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?

No.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A.

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

N/A.

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

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

Scott C. Safian
Director, Enforcement & Litigation Division
Office of Investigation, Enforcement & Audit
355 E St., SW
Washington, DC 20024

Marvin Lykes
Chief Information Security Officer
1400 Independence Ave., SW
Washington, DC 20250

Elamin Osman
Chief Information Officer
1400 Independence Ave., SW
Washington, DC 20250

Privacy Office
Room 2168, South Building
Washington, DC 20250

Approval Signatures

Barring any major changes, no signatures are required before the ATO expiration date on 03/28/2022.