USDA Privacy Impact Assessment

Fiscal Year 2025

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Table of Tables

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	AssuranceNet (ANet)
Program Office	Office of the Chief Information Officer
Mission Area	FSIS
CSAM Number	1110
Date Submitted for Review	9/24/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Keith Komosinski	(863) 220-4182
Information System Security Manager	Marvin Lykes	(202) 515-6115
System/Program Managers	Ryan Cast	(949) 244-6706

Abstract

This document serves as the Privacy Impact Assessment (PIA) for the United States Department of Agriculture (USDA) AssuranceNet (ANet). 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. ANet is classified as a privacy sensitive system and therefore requires a PIA.

Overview

The AssuranceNet (ANet) boundary consists of two web-based applications that support the USDA (United States Department of Agriculture) FSIS (Food Safety Inspection Service) in their efforts to monitor, analyze, and report the nation’s commercial supply of meat, poultry, and egg products - ensuring that the products are safe, packaged, and correctly labeled. The applications are Meat and Poultry Handlers (MPH) and AssuranceNet (ANet).

Meat and Poultry Handlers (MPH) is a web-based application that registers firms with the USDA if they deal in meat or poultry products or siluriform in or for commerce (between any State or territory designated for 21 U.S.C. 643 and/or 21 U.S.C. 460 or the District of Columbia), unless a firm operates under Federal Inspection.

ANet, built on the Open Liberty Platform, supports the Office of Field Operations (OFO), the Office of Investigation, Enforcement & Audit (OIEA), and the Office of Administrator and Internal Affairs (OAIA). ANet transforms near-real-time performance data into valuable decision-making information for managers daily. Report data is extrapolated from various FSIS databases and applications, as well as from manual data entry within ANet. This centralized system enables supervisors and senior managers to create custom reports that help monitor industry compliance in FSIS's program areas.

The ANet system has four module categories: In-Commerce System (ICS) Modules, Assessment Modules, Misconduct Modules, and Litigation Modules.

- The In-Commerce System (ICS) modules include activities such as surveillance (food safety and food defense); product control (detention and seizure), investigation, and case management.
- The Assessment module provides leadership with the ability to generate reports to determine enforcement actions, non-supervisory plant personnel performance, and the knowledge and skills of field supervisory personnel.
- The Misconduct module includes records on employee misconduct investigations and inquiries.
- The Litigation module contains case information regarding labor and employment hearings and appeals.

The modules and their sections are described in more depth below:

Table 1: In-Commerce Module (ICS)

Sub-system	Program/Business Area	Description
Firm Information Records	OIEA, OFO	Firm Information records stores items like: • Firm (business) name • Business type • Business tier • Registration information • Physical address • State • County • Latitude/Longitude • Hours of operation • Product information • Organization structure • Names of firm owners • Managing officials • Firm history (with hyperlinks to surveillance) • Product control • Investigations • Firm enforcement records
Surveillance Records	OIEA	Surveillance contains findings on firms and businesses that have previously violated or are potential violators of the Federal Meat Inspection Act (FMIA), Egg Products Inspection Act (EPIA), andPoultry Products Inspection Act (PPIA), which administrative, criminal, or civil action may be taken. The findings include an evaluation of the firm's food safety and food defense activities, as well as an assessment of other FSIS food safety standards. Surveillance information includes food defense information from: • FSIS Form 5420-3 Food3 Defense Surveillance Findings Sensitive Security Information • Any additional information that is captured during activities that support FSIS Directive 8010.1, Methodology for Conducting Surveillance Activities.

Sub-system	Program/Business Area	Description
Product Control Records	OIEA	Product Control records contain information obtained from: • FSIS Form 8080.1 – Notice of Detention • FSIS Form 8080.6 – Personal Use • FSIS Form 8400-1 – Notice of Termination of Detention • FSIS Form 8080.4 Voluntary Destruction of Human Food Notice using the standard methodology outlined in Directive 8410.1 – Detention and Seizure.
Investigation Records	OIEA	Investigation records contain information about OIEA and state program investigations. Investigation records contain information from: • FSIS Form 8000-17 – Evidence Receipt and Chain of Custody • FSIS Form 8000-16 – Evidence Log • FSIS Form 8000-7 – Exhibit Cover Sheet. Investigation records include any additional information that is captured during OIEA Compliance and Investigation Division (CID) investigative activities that support: • FSIS Directive 8010.2 Investigative Methodology • FSIS Directive 8010.3 Procedures for Evidence Collection, Safeguarding, and Disposal.
Enforcement Records	OIEA	Enforcement contains records of actions FSIS has taken against a firm. Program employees capture data to review and track cases, determining the appropriate criminal, civil, or administrative enforcement action. This includes: • Associated investigation information • Associated AER information • Program actions • Office of General Counsel actions • United States Attorney's Office actions • Violator information and dispositions

Table 2: Assessment Modules

Sub-System	Program/Business Area	Description
Administrative Enforcement Reports (AER) Records	OFO, OIEA	AER is used to maintain an electronic record of enforcement actions, including: • FSIS Form 5400-9 Administrative Enforcement Report • Files representing the exhibits supporting the action • Establishment responses and submitted documents Agency-generated documentation relevant to the case (e.g., requests to the establishment for clarification, verification plans).
In-Plant Performance System (IPPS) Records	OFO	IPPS is a tool that OFO supervisors use to assess the performance of non-supervisory personnel in the in-plant inspection program. IPPS covers all non-supervisory in-plant inspection program personnel, including: • Food Inspectors • Consumer Safety Inspectors • Public Health Veterinarians. In addition, IPPS provides the opportunity for first-hand, onsite observation of how well an employee conducts FSIS inspection and verification procedures in federally inspected establishments.
Supervisory Tool for Assessment Results (STARS) Records	OFO	Supervisors use STARS to assess the knowledge and proficiency of field-level supervisory personnel. It requires supervisory personnel to determine whether in-plant, subordinate supervisors carry out both program activities and supervisory responsibilities, in accordance with applicable regulatory requirements and FSIS directives and notices.

Table 3: Misconduct Modules

Sub-System	Program/Business Area	Description
Misconduct Investigation Records	OA Internal Affairs	Misconduct Investigation records contain case information regarding employee misconduct investigations and inquiries. These records include: • Complaints formally investigated by IA • Referred cases to other internal program areas. The Program Employee/Deputy Director/Director electronically documents key activities by entering data in different fields, including relevant case information. Relevant case information contains information from: • FSIS Form 8000-17 – Evidence Receipt and Chain of Custody • FSIS Form 8000-16 – Evidence Log and • FSIS Form 8000-7 – Exhibit Cover Sheet The completion of employee misconduct investigations requires forwarding pertinent case documents to the FSIS Labor and Employee Relations Division (LERD) for further review and any disciplinary action they deem necessary. In some instances, cases may be referred to OIG or handled by other FSIS program areas.

Table 4: Litigation Modules

Sub-System	Program/ Business Area	Description
Hearing and Appeals Branch (HAB) Records	OIEA Litigators	Hearings and Appeals (HAB) records contain case information regarding: • Labor and employment • Litigation activities • Reporting components These records include cases litigated before the Equal Employment Opportunity Commission (EEOC), Merit System Protection Board (MSPB), Arbitration, and other third parties. Staff documents key activities by entering data regarding: • Relevant case information • Case dispositions • Associated litigation costs The reporting tool in this system is used to aid in assessing case trends, performance, and outcomes. In some instances, cases may be referred to OGC or handled by the U.S. Attorney when individuals file lawsuits in Federal courts. The HAB Component also tracks other critical items such as: • Freedom of Information Act (FOIA) Records • Subpoenas • Suspension and Debarment cases for the purpose of reporting Division activities and accomplishments.

Section 1: Authorities and Other Requirements

These questions identify all statutory and regulatory authorities for operating the project, application, or system, including the authority for collection, which SORN applies, if an ATO has been completed, and if there is Paperwork Reduction Act coverage:

What legal authorities and/or agreements permit the collection of information by the project, application, or system?

The legal authority to collect information is provided in the ANet SORN. They are described as follows: Poultry Products Inspection Act (21 U.S.C. 451 et seq.); Federal Meat Inspection Act (21 U.S.C. 601 et seq.); Egg Products Inspection Act (21 U.S.C. 1031 et seq.); Humane Methods of Livestock Slaughter Act of 1978 (7 U.S.C. 1901–1906); Authority to Operate (ATO), dated 03/23/2017.

Has Authorization and Accreditation (A&A) been completed for the project, application, or system?

The legal authority to operate Anet is provided by the signed Authority to Operate (ATO) letter dated 02/24/2025.

Which System of Records Notices (SORNs) apply to the information?

AN SORN: USDA/FSIS-0005 - AssuranceNet (AN) - 87 FR 16163 - March 22, 2022

AN Exemption: USDA/FSIS-0005-AssuranceNet (AN) – Exemption – 89 FR 12745 – February 20, 2024

Is the collection of information covered by the Paperwork Reduction Act?

No

Section 2: Information Characterization

These questions define the scope of the information requested and collected, as well as the reasons for its collection as part of the project, application, or system being developed:

What information is collected, used, disseminated, or maintained in the project, application, or system?

Identifying Numbers:

- File or Case ID Number
- Employee Identification Number
- Personal Mobile Phone Number
- Business Mobile Phone Number (Sole Proprietor)

Biographical Information:

- Name (Including Nicknames)
- Business Mailing Address (Sole Proprietor)
- Business Phone or Fax Number (Sole Proprietor)
- Home Phone or Fax Number
- Home Address
- ZIP Code
- Business Email Address
- Global Positioning System (GPS) or Location Data

Distinguishing Features:

- Signatures

Specific Information and File Types:

- Case Files

What are the sources of the information in the project, application, or system?

The sources of information in the system are:

- FSIS System (Public Health Information System)
- Individuals (USDA and State)

How is the information collected?

The information is collected by:

- FSIS System
  - Public Health Information System (PHIS), which provides establishment profiles in Anet.
- Individuals
  - District personnel (inspector) assigned to an establishment

- Investigators (FSIS and State) who conduct in-commerce surveillance and investigation
- Investigators (FSIS only) who conduct misconduct investigations

Does the project, application, or system use information from commercial sources or publicly available data? If so, explain why it is used.

ANet does not use information that comes from commercial sources or publicly available data.

How will the information be checked for accuracy? How often will it be checked?

Establishment profiles are checked using a daily data feed from PHIS. All other data is verified by the establishment and commerce after the investigation or surveillance is conducted. Investigations or surveillance are conducted on a quarterly or annual basis.

Does the project, application, or system use third-party websites?

No

What is the purpose of the use of third-party websites?

ANet does not have any third-party websites.

What PII will be made available to the agency though the use of third-party websites?

ANet does not have any third-party websites.

List the privacy risks and mitigations related to the characterization of the information.

Privacy Risk: AssuranceNet contains Personal Identifiable Information (PII) that can identify an individual, their job performance, and any misconduct investigations (if applicable). If PII is mischaracterized, it can inadvertently be supplied to unauthorized individuals.

Mitigation: ANet itself is strictly controlled, allowing only those with a USDA-approved secure single sign-on application (eAuth – Level 2 Access) and an ANet role to access ANet. ANet cannot be accessed without an authorized account. Users are assigned roles based on their job functions, which determine their level of access. ANet 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. Only designated users can add or modify establishment or user information and are responsible for ensuring that PII is accurate.

Section 3: Information Uses

These questions delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated and/or maintained will support the project, application, or system's business purpose.

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.

Does the project, application, or system use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No.

List the privacy risks and mitigations related to uses of the information.

Privacy Risk: Information within ANet could be used for unintended purposes or accessed by unauthorized users.

Mitigation: All USDA employees must pass a Government National Agency Check with Inquiries (NACI) background check prior to being granted system access. USDA Contractors are governed by contracts that identify the rules of behavior for USDA, FSIS systems, and security. Contracts are reviewed upon renewal by management and contract personnel experts. All USDA users (employees or contractors) are required to complete recurring security and privacy training, which is conducted through the Office of the Chief Information Officer.

All authorized staff using the system must comply with the Agency's general Information Technology Use Policy. Rules of behavior and consequences, as well as system use notifications, are in accordance with the Privacy Act, subsection e [9].

ANet itself is strictly controlled, allowing only those with a USDA-approved secure single sign-on application (eAuth – Level 2 Access) and an ANet role to access ANet. ANet cannot be accessed without an authorized account. Users are assigned roles based on their job functions, which determine their level of access. ANet's 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.

Regardless of role, all user activity (i.e. user logins and changes made) is captured and logged. This allows administrators to identify the source of any incorrect or incomplete data recorded in the system.

ANet has security safeguards, boundary protection devices, proxy servers, application gateways, intrusion prevention/detection, etc. ANet leverages host firewalls for controlling access between the tiered layers. Traffic is also monitored for malicious content, unauthorized

access, inside threats, and exfiltration. Any Data in transit is protected using Transport Layer Security (TLS).

Section 4: Notice

These questions are intended to provide notice to the individual of the scope of information collected, the right to consent to use of the information, and the right to decline to provide information.

How does the project, application, or system provide notice to individuals prior to collection?

Notice is provided to the FSIS employees at the time of hiring. Plant vendors are notified during the business agreement process. In accordance with Directive 8010.2, 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. It is not necessary to provide an FSIS employee with a copy of the Privacy Act Notice.

For the PII that is collected within ANet's boundary, users are notified using a privacy link as well as a consent banner, and all individuals are notified using the PIA and SORN. For ANet & MPH users, the consent banner is displayed before an individual accesses the Anet boundary, and the user must provide permission to use their PII by selecting "Accept." Once a user is within the ANet boundary, a link to the USDA's privacy policy is included at the bottom of the page, which provides details on data collection practices.

What options are available for individuals to consent, decline, or opt out of the project?

If a user does not grant ANet/MPH permission to use their PII within the consent banner, they will not be provided with access to the ANet boundary.

FSIS published a rule to exempt certain investigatory records maintained by the ANet system of records from the notification and access provisions of the Privacy Act under 5 U.S.C. 552a(c)(3), (d)(1)–(4), (e)(1) (e)(4)(G)–(I), and (f) (87 FR 16105). FSIS explained that ANet includes investigatory material compiled for law enforcement, which fall under the Privacy Act exemptions in 5 U.S.C. 552a(k). FSIS also explained that the exemptions were necessary to protect information on the methods used in law enforcement activities from those individuals who are subjects to the investigation and the identities and physical safety of witnesses and others who aid in investigations. Moreover, FSIS explained that the exemptions would ensure FSIS' ability to obtain information from third parties and safeguard those investigatory records that are needed for litigation (87 FR 16105–16106). For more detailed information, see Privacy Act Exemption for AssuranceNet.

List the privacy risks and mitigations related to notice.

Privacy Risk: Those whose information resides in the ANet boundary may be unaware that their data is being collected due to insufficient notice.

Mitigation: The PII within the ANet boundary is authorized by the legal authority mentioned in section 1.1, and only the PII that is authorized is processed within the boundary. If information is collected within the ANet boundary, users are notified using both a privacy link and a consent banner. All individuals are notified using PIA and SORN.

FSIS published a rule to exempt certain investigatory records maintained by the ANet system of records from the notification and access provisions of the Privacy Act under 5 U.S.C. 552a(c)(3), (d)(1)–(4), (e)(1) (e)(4)(G)–(I), and (f) (87 FR 16105). FSIS explained that ANet includes investigatory material compiled for law enforcement, which falls under the Privacy Act exemptions in 5 U.S.C. 552a(k). FSIS also explained that the exemptions were necessary to protect information on the methods used in law enforcement activities from those individuals who are subjects of the investigation, as well as the identities and physical safety of witnesses and others who aid in investigations. Moreover, FSIS explained that the exemptions would ensure FSIS's ability to obtain information from third parties and safeguard those investigatory records necessary for litigation (87 FR 16105–16106). For more detailed information, see Privacy Act Exemption for AssuranceNet.

Section 5: Data Retention

These questions outline how long information will be retained after the initial collection.

What information is retained and for how long?

ANet tracks, measures, and monitors the performance of the key public health functions of inspection, verification, surveillance, enforcement. As such, ANet must keep all information indefinitely for legal purposes.

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, indicate the name of the records retention schedule.

ANet has specific exemptions: AN Exemption: USDA/FSIS-0005-AssuranceNet (AN) – Exemption – 89 FR 12745 – February 20, 2024. This exemption allows information within the ANet boundary to be retained indefinitely for legal purposes due to its investigatory nature.

List the privacy risks and mitigations related to data retention. Follow this format:

Privacy Risk: ANet maintains records to ensure access to historical records for legal purposes. Since information is kept, a significant amount of information can be accessed in the event of a breach.

Mitigation: ANet has been provided with the authority (see section 1.0) to collect all necessary information to achieve ANet's purpose and does not collect any information that is not relevant to its purpose.

ANet itself is strictly controlled, allowing only those with a USDA-approved secure single sign-on application (eAuth – Level 2 Access) and an ANet role to access ANet. ANet cannot be accessed without an authorized account. Users are assigned roles based on their job functions, which determine their level of access. ANet 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.

Regardless of role, all user activity (i.e., user logins and changes made) is captured and logged. This allows administrators to identify the source of any incorrect or incomplete data recorded in the system.

In addition, ANet has security safeguards, boundary protection devices, proxy servers, application gateways, intrusion prevention/detection, etc. ANet leverages host firewalls for controlling access between the tiered layers. Traffic is also monitored for malicious content, unauthorized access, inside threats, and exfiltration. Any Data in transit is protected using Transport Layer Security (TLS).

Section 6: Information Sharing

These questions define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared, received, and/or transmitted? What information is shared, received, and/or transmitted, and for what purpose? How is the information transmitted?

ANet connects internally to the following applications:

- ICAM for E-Auth services
- PHIS to receive establishment profiles
- FRT to provide data for reporting purposes.

Based on request, ANet may be shared with USDA entities (e.g. OIG) who have a need-to-know.

List the privacy risks and mitigations related to internal information sharing and disclosure. Follow this format:

Privacy Risk: Individuals who do not have a need-to-know can accidentally acquire information that is within ANet.

Mitigation: All USDA employees must pass a Government National Agency Check with Inquiries (NACI) background check prior to being granted system access. USDA Contractors are governed by contracts that identify the rules of behavior for USDA, FSIS systems, and security. Contracts are reviewed upon renewal by management and contract personnel experts. All USDA users (employees or contractors) are required to complete recurring security and privacy training, which is conducted through the Office of the Chief Information Officer.

All authorized staff using a system must comply with the Agency's general Information Technology Use Policy. Rules of behavior and consequences, as well as system use notifications, are in accordance with the Privacy Act, subsection e [9], and OMB Circular A-130.

ANet itself is strictly controlled, allowing only those with a USDA-approved secure single sign-on application (eAuth – Level 2 Access) and an ANet role to access ANet. ANet cannot be accessed without an authorized account. Users are assigned roles based on their job functions, which determine their level of access. ANet 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.

Regardless of role, all user activity (i.e., user logins and changes made) is captured and logged. This allows administrators to identify the source of any incorrect or incomplete data recorded in the system.

With which external organizations (outside USDA) is information shared, received, and/or transmitted? What information is shared, received and/or transmitted, and for what purpose? How is the information transmitted?

Information is not shared externally.

List the privacy risks and mitigations related to external information sharing and disclosure.

Privacy Risk: Not Applicable.

Mitigation: Not Applicable.

Section 7: Redress

These questions address the individual's ability to ensure the accuracy of the information collected about him or her.

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, unless covered by exemption (referenced below).

Please note that Anet has specific exemptions: AN Exemption: USDA/FSIS-0005-AssuranceNet (AN) – Exemption – 89 FR 12745 – February 20, 2024

"On March 22, 2022, FSIS published a system of records notice (SORN) for USDA/FSIS–0005, ANet (87 FR 16163). In the same Federal Register, FSIS published a proposed rule to exempt certain investigatory records maintained by the ANet system of records from the notification and access provisions of the Privacy Act under 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(1) (e)(4)(G)–(I), and (f) (87 FR 16105). FSIS explained in the proposed rule that ANet includes investigatory material compiled for law enforcement, which falls under the Privacy Act exemptions in 5 U.S.C. 552a(k). FSIS also explained that the proposed exemptions were necessary to protect information on the methods used in law enforcement activities from those individuals who are subjects of the investigation, as well as the identities and physical safety of witnesses and others who aid in investigations. Moreover, FSIS explained that the exemptions would ensure FSIS's ability to obtain information from third parties and safeguard those investigatory records that are needed for litigation (87 FR 16105–16106)."

FSIS FOIA Officer at FSIS Freedom of Information Act Office Room 1175- South Building, 14th and Independence Avenue, SW, Washington, DC 20250-3700 - Phone: (202) 720-2109- Fax (202) 690-3023 – E-mail: fsis.foia@usda.gov.

For more information about how to make a FOIA request, see FSIS Freedom of Information Act

What are the procedures for correcting inaccurate or erroneous information?

Based on the ANET SORN (FSIS-2011-0031): "In accordance with the 7 CFR part 1, individuals seeking to contest or amend information maintained in the system should direct their request to the above listed System Manager and should include the reason for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. A request for contesting records should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information."

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

Based on the ANET SORN (FSIS-2011-0031): "Because individual access to these records would impair investigations and alert subjects that their activities are being scrutinized, the Agency proposes to exempt portions of this system from the notification and access procedures of the Privacy Act, pursuant to section (k)(2) and USDA's implementing regulations at 7 CFR part 1. However, individuals seeking notification of and access to their records should submit a written request, with reasonable specificity, to the FSIS Freedom of Information Act (FOIA)

Office at: 1400 Independence Ave. SW, Room 1168-South, Mail Stop No. 3713, Washington, DC 20250. Requests for such access will be reviewed on a case-by-case basis."

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

Based on the ANET SORN (FSIS-2011-0031): "In accordance with the 7 CFR part 1, individuals seeking to contest or amend information maintained in the system should direct their request to the above listed System Manager and should include the reason for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. A request for contesting records should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information."

List the privacy risks and mitigations related to redress.

Privacy Risk: Individuals whose information is stored in ANet may be unaware of how to verify the accuracy of the information collected about them.

Mitigation: In accordance with the 7 CFR part 1, individuals seeking to contest or amend information maintained in the system should direct their request to the above listed System Manager and should include the reason for contesting it and the proposed amendment to the information with supporting information to show how the record is inaccurate. A request for contesting records should contain: Name, address, ZIP code, name of the system of records, year of records in question, and any other pertinent information.

Section 8: Auditing and Accountability

These questions describe technical safeguards and security measures:

How is the information in the project, application, or system secured?

All USDA employees must pass a Government National Agency Check with Inquiries (NACI) background check prior to being granted system access. USDA Contractors are governed by contracts that identify the rules of behavior for USDA, FSIS systems, and security. Contracts are reviewed upon renewal by management and contract personnel experts. All USDA users (employees or contractors) are required to complete recurring security and privacy training, which is conducted through the Office of the Chief Information Officer.

All authorized staff using a system must comply with the Agency's general IT use policy. Rules of behavior and consequences, as well as system use notifications, are in accordance with the Privacy Act, subsection e [9], and OMB Circular A-130.

ANet itself is strictly controlled, allowing only those with a USDA-approved secure single sign-on application (eAuth – Level 2 Access) and an ANet role to access ANet. ANet cannot be accessed without an authorized account. Users are assigned roles based on their job functions, which determine their level of access. ANet 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.

Regardless of role, all user activity (i.e., user logins and changes made) is captured and logged. This allows administrators to identify the source of any incorrect or incomplete data recorded in the system.

Anet is hosted in Azure. Access control lists are implemented between layers of user security safeguards, boundary protection devices, proxy servers, application gateways, intrusion prevention/detection, etc. Azure firewalls are leveraged for controlling access between the tiered layers. Azure Defender is also used to monitor traffic for malicious content, unauthorized access, insider threats, and exfiltration. See the diagrams in the system description of the SSP.

What procedures are in place to determine which users may access the project, application, or system, and are they documented?

ANet is strictly controlled by only allowing those with a USDA-approved secure single sign-on application (eAuth – Level 2 Access) and an ANet role access to ANet. ANet cannot be accessed without an authorized account. Users are assigned level-of-access roles based on their job functions. ANet 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.

How does the project, application, or system review and approve information sharing requirements?

All internal connections are documented within the System Security Plans, which are reviewed and approved by the System Owner on an annual basis as part of the accreditation and assessment process.

Describe what privacy training is provided to users either generally or specifically relevant to the project, application, or system.

All required training is conducted online through AgLearn or via an external online training link for users who do not yet have a network account. All new hires must complete the USDA Information Security Awareness Training (ISAT) through the public Course Avenue website. Security and privacy training is required during the onboarding process as well as on an annual basis.

Security Awareness Training details current security awareness concerns, relevant cybersecurity information, procedures when using government equipment and the internet, and outlines the rules and behaviors that all users are expected to uphold and follow.

Personally Identifiable Information (PII) Training provides an in-depth understanding of Personally Identifiable Information (PII). The course covers how to manage PII if it is lost, compromised, or disclosed. In addition, it provides examples of non-PII, identifies who is responsible for PII, outlines past PII incidents, explains PII policy, provides guidance on protecting PII, describes how to encrypt documents, and explains how to report PII Incidents.

Users have 90 days to complete the mandatory annual Information Security Awareness Training. Failure to complete the training will result in restricted access to the network. The course, pre-test, and assessment are available on the Department of Agriculture Learning Management System (AgLearn).

Training is tracked through AgLearn. FSIS can generate reports as needed to provide updates on the percentage of the total FSIS universe that has completed ISAT for that fiscal year and show which users are late or non-compliant.