USDA Privacy Impact Assessment

Fiscal Year 2024

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

Privacy Impact Assessment for the USDA IT System/Project.. 3

Mission Area System/Program Contacts.. 3

Abstract.. 4

Overview.. 4

Section 1: Authorities and Other Requirements 7

Section 2: Characterization of the Information 8

Section 3: Uses of the Information.. 13

Section 4: Notice 15

Section 5: Data Retention... 17

Section 6: Information Sharing 19

Section 7: Redress 21

Section 8: Auditing and Accountability 22

Privacy Impact Assessment Review 23

Signature of Responsible Officials... 23

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Electronic Management of National Environmental Policy Act (eMNEPA)
Program Office	Ecosystem Management Coordination
Mission Area	Natural Resource Environment Forest Service (NRE FS)
CSAM Number	2408
Date Submitted for Review	06/04/2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Benjamin J. Moreau	benjamin.moreau@usda.gov	202-720-3463
Information System Security Manager	Kristopher Harig	kristopher.harig@usda.gov	208-387-5170
System/Program Managers	Judy Suing	judy.suing@usda.gov	385-226-6448

Abstract

The abstract provides the simplest explanation for the "what does the system do?" and will be published online to accompany the PIA link.

The Electronic Management of National Environmental Policy Act (eMNEPA) Program is maintained by the U.S. Department of Agriculture (USDA) Forest Service (FS) to reduce the workload associated with NEPA compliance using electronic communication and improved process management. The mission is to reduce the field's administrative burden and improve its effectiveness at completing NEPA by supporting compliance, efficiency, and sustaining knowledge. eMNEPA's purpose is to improve the effectiveness and efficiency of NEPA compliance activities within FS projects. To accomplish it's function eMNEPA utilizes four applications Planning, Appeals, and Litigation System (PALS), Comment Analysis and Response Application (CARA), Datamart, and Mailing List Management (MLM); these applications collect and store Personal Identifiable Information (PII) for business use to reduce the workload associated with NEPA compliance and improved process management.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

The eMNEPA Program is one of the U.S. Department of Agriculture (USDA) Forest Service (FS) e-Government (e-Gov) initiatives. It is an incremental process modernization program, not a single tool or application. The eMNEPA program began in 2004 as an effort to reduce the workload associated with the National Environmental Policy Act (NEPA) compliance using electronic communication and improved process management. The mission is to reduce the field's administrative burden and improve its effectiveness at completing NEPA by supporting compliance, efficiency, and sustaining knowledge. Its purpose is to improve the effectiveness and efficiency of NEPA compliance activities within FS projects.

The eMNEPA Program is comprised of four applications that interact with PII:

Planning, Appeals, and Litigation System (PALS) - PALS' purpose is to track NEPA project data and status. Information is collected via internal FS users utilizing PALS to input project information, dates, documents, and litigation information to provide a paper trail of NEPA actions to comply with NEPA regulations. eMNEPA consumes the planning project information from this application. PALS collects and stores PII including:

- Federal employees or Federal contractors input first name, last name, phone number, email address, file and case identification number, and docket number of litigants and appellants information received from the Department of Justice, USDA Office of General Counsel or Public Access to Court Electronic Records (PACER).
- ICAM Shared Services transmit account information including first name, last name, and e-Auth ID.

Comment Analysis and Response Application (CARA) - CARA is the Agency's web-based solution for receiving, analyzing, and responding to public comments and objections. CARA reduces processing time and cost through automation and standardization and facilitates sharing of information across the Agency and with the public. It automates form management and mailing lists updates. It connects to the public web with a standard webform and public reading rooms. CARA's purpose is to track public comments including legal objections for NEPA projects and directives. The information supports the business purpose for legal objections to be considered valid. CARA collects and stores PII including:

- Members of the public (U.S. citizens) provide first name, last name, mailing address, email address via web form.
- Federal employees or Federal contractors input first name, last name, mailing address, email address via web form.Comment Analysis and Response Application (CARA)

Datamart - Datamart's purpose is to share and synchronize data between PALS and CARA. Datamart's information supports business purpose by serving as a Web API to provide data points to display on the public web for PS project pages. Datamart collects and stores PII including:

- DataMart receives from PALs eAuth ID, first name, last name, phone number, email address, project contact information; first name, last name, phone number, email address.

Mailing List Management (MLM) - MLM. It consists of the MLM application integrated with GovDelivery which is a software as a service solution. The system allows Forests to automate communications and allows the public to sign up for the types of information that they want to receive. It enables the public to manage their own mailing list preferences and Forests/Districts to more easily send out NEPA notifications and project information to the public. MLM contains names, contact information, and interests of engaged members of the public. MLM promotes early public input, proactive collaboration, better decisions, and public acceptance. MLM collects and stores PII. MLM's purpose is to manage public user communications regarding projects in PALS. MLM's information supports the business purpose by serving as a conduit to manage mailing lists.

- Members of the public (U.S. citizens) provides first name, last name, and mailing address via web form at https://data.fs2c.usda.gov/mlm/ or uploaded via GovDelivery.

Section 1: Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

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

NATIONAL ENVIRONMENTAL POLICY ACT OF 1969 [(Public Law 91–190)] [As Amended Through P.L. 118–5, Enacted June 3, 2023]
Code of Federal Regulations – Title 7: Agriculture – 7 CFR 1.27
Code of Federal Regulations – Title 40: Public Involvement – 40 CFR 1506.6
Freedom of Information Act (Public Law 89-554, 80 Stat. 383; Amended 1996, 2002, 2007, 2016)
Wyoming Outdoor Council vs. Forest Service, 1996.

1.2. Has Authorization and Accreditation (A&A) been completed for the system?

Yes

1. The System Security Plan Status, Approved.

2. The System Security Plan Status Date: 3/12/2025

3. The Authorization Status, Approved.

4. The Authorization Date: 3/12/2025

5. The Authorization Termination/Expiration Date: 3/12/2028

6. The Risk Review (Risk Assessment) Completion Date: 4/3/2025

7. The FIPS 199 classification of the system MODERATE.

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

All of the data collected falls under:

USDA/OCX - AskUSDA Contact Center – 88 FR 45882

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

No.

Section 2: Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers

☐ Social Security number	☐ Truncated or Partial Social Security number	☐ Driver's License number
☐ Passport number	☐ License Plate number	☐ Registration number
☒ File/Case ID number	☐ Student ID number	☐ Federal Student Aid number
☐ Employee Identification number	☐ Alien Registration number	☐ DOD ID number
☐ Professional License number	☐ Taxpayer Identification number	☐ Business Taxpayer Identification number (sole proprietor)
☐ Credit/Debit Card number	☐ Business Credit Card number (sole proprietor)	☐ Vehicle Identification number
☐ Business Vehicle Identification number (sole proprietor)	☐ Personal Bank Account number	☐ Business Bank Account number (sole proprietor)
☐ Personal Device Identifiers or Serial numbers	☐ Business Device Identifiers or Serial numbers (sole proprietor)	☒ Personal Mobile number

☐ Health Plan Beneficiary number

☒ Business Mobile number (sole proprietor)

☐ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)

☐ Ethnicity

☐ City or County of Birth

☐ Citizenship

☒ Home Address

☐ Spouse Information

☐ Race

☒ Personal Email Address

☐ Employment Information

☐ Education Information

☐ Professional/Personal References

☒ Business Mailing Address (sole proprietor)

☒ Business Phone or Fax Number (sole proprietor)

☐ Group Organization/Membership

☐ Immigration Status

☒ ZIP Code

☐ Children Information

☐ Nationality

☒ Business Email Address

☐ Alias (Username/Screenname)

☐ Resume or Curriculum Vitae

☐ Date of Birth (MM/DD/YY)

☐ Country of Birth

☐ Religion/Religious Preference

☒ Home Phone or Fax Number

☐ Marital Status

☐ Military Service Information

☐ Mother’s Maiden Name

☐ Global Positioning System (GPS)/Location Data

☐ Personal Financial Information (Including loan information)

☐ Business Financial Information (Including loan information)

Biometrics

☐ Fingerprints

☐ Retina/Iris Scans

☐ Hair Color

☐ Video Recording

☐ DNA Sample or Profile

Distinguishing Features

☐ Palm Prints
☐ Dental Profile
☐ Eye Color
☐ Photos
☐ Signatures

Characteristics

☐ Vascular Scans
☐ Scars, Marks, Tattoos
☐ Height
☐ Voice/Audio Recording
☐ Weight

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)
☐ Cell Tower Records (e.g., Logs, User Location, Time)
☐ Network Communication Data

Medical /Emergency Information

☐ Medical/Health Information
☐ Workers' Compensation Information
☐ Mental Health Information
☐ Patient ID Number
☐ Disability Information
☐ Emergency Contact Information

Specific Information/File Types

☐ Personnel Files
☐ Health Information
☒ Case Files
☐ Law Enforcement Information
☐ Academic/Professional Background Information
☐ Security Clearance/Background Check
☐ Credit History Information
☐ Civil/Criminal History Information/Police Record
☐ Taxpayer Information/Tax Return Information

List additional information collected but not listed above here (for example, a personal phone number that is used as a business number):

e-Authentication (e-Auth) identification number (ID), Docket Number

2.2. What are the sources of the information in the system/program?

Planning, Appeals, and Litigation System (PALS)

- Federal Employees and Federal Contractors: documentation First name, last name, phone number, email address, file and case identification number, and docket number of litigants and appellants information is received from the Department of Justice, USDA Office of General Counsel or Public Access to Court Electronic Records (PACER). eAuth ID is received from ICAM Share Services.

Comment Analysis and Response Application (CARA)

- Members of the public (U.S. citizens) provide first name, last name, mailing address, email address via web form.
- Federal employees or Federal contractors input first name, last name, mailing address, email address via web form.

Datamart

- Retrieves the following PII from PALS: eAuth ID, first name, last name, phone number, email address, project contact information
-

Mailing List Management (MLM)

- Members of the public (U.S. citizens) provides first name, last name, and mailing address via web form at https://data.fs2c.usda.gov/mlm/ or uploaded via GovDelivery.

Note: MLM, ServiceBroker, eFile interact with information from DataMart

2.2.1. How is the information collected?

Planning, Appeals, and Litigation System (PALS)

- PII is received electronically.

Comment Analysis and Response Application (CARA)

- PII is received electronically via web form.

Datamart

- PII is received electronically via PALS.

Mailing List Management (MLM)

- PII is received electronically via web from or GovDelivery.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

No

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

The eMNEPA system allows the public to provide accurate, inaccurate or no personal information at all with their comments. All comments are accepted per the NEPA process regardless of the quality or existence of contact information. The contact information is collected to fulfill legal requirements and to contact individuals if they request to be contacted. The NEPA program does not validate publicly provided contact information. Responsibility for accuracy for the PII received from the ICAM, Department of Justice, USDA Office of General Counsel or Public Access to Court Electronic Records (PACER.) relies on the provider. The responsibility is on the information provider to ensure that the information is correct. This applies to all eMNEPA applications.

2.5. Does the system/program use third-party websites?

No

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

N/A

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

N/A

2.6. **Privacy Impact Analysis**: Related to characterization of the information.

Follow the format below:

Privacy Risk: Incorrectly categorizing PII can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Mitigation:

Privacy risks are mitigated in the following manner:

- Only authorized and authenticated users have access to the system.
- Least privilege access.
- EAuth is being used to authenticate users where possible.
- Sensitive data is encrypted in transit.
- Sensitive data is encrypted at rest where possible; and
- Monitoring the security of the system on a continuous basis.

Section 3: Uses of the Information

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

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

Planning, Appeals, and Litigation System (PALS)
PALS' purpose is to track NEPA project data and status. Information is collected via internal FS users utilizing PALS to input project information, dates, documents, and litigation information to provide a paper trail of NEPA actions to comply with NEPA regulations.

Comment Analysis and Response Application (CARA)
CARA's purpose is to track public comments including legal objections for NEPA projects and directives. The information supports the business purpose for legal objections to be considered valid.

Datamart
Datamart's purpose is to share and synchronize data between PALS and CARA. Datamart's information supports business purpose by serving as a Web API to provide data points to display on the public web for PS project pages.

Mailing List Management (MLM)
MLM's purpose is to manage public user communications regarding projects in PALS. MLM's information supports the business purpose by serving as a conduit to manage mailing lists.

3.2. Does the system/project/program 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.

Analysis tools are not part of nor provided by eMNEPA.

3.3. **Privacy Impact Analysis**: Related to uses of the information.

Follow the format below:

Privacy Risk:

If PII is used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

Mitigation: eMNEPA collects and uses only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

Inform individuals about how their personal information will be used, including any potential secondary uses, through clear and accessible privacy notices.

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

Public project notices inform the general public of the opportunity to comment and contain a warning that information provided by the public is retained by the Forest Service in the project record.

The public comment web form contains a warning that contact information provided in the contact form fields is not publicly visible but is retained as part of the project record, and information entered into the comment text box is publicly available.

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

Public project announcements and the public comment web form state that information provided by the public will become part of the permanent project record. Individuals who do not consent to this use may submit anonymous comments. When people submit a request to be contacted with further information about the project, their contact information may be added to a project mailing list in GovDelivery or eMNEPA specific to that project.

Yes. Public project announcements in the newspaper of record for regional, forest and district-level projects state that contact information is not required to comment; contact information is required only to retain legal standing to object to the project. Individuals routinely provide anonymous comments for consideration without supplying any PII. All contact information text fields in the comment web form are optional and do not need to be completed to submit comments. This is indicated by not having asterisks next to contact information fields and by the warning above the letter text entry box which states, “Do not enter any personally identifiable information (PII) such as address or email in the text editor below. Your name and all information entered into the text box below may be published on this website. Enter contact information in the form fields above.”

4.3. **Privacy Impact Analysis**: Related to notice.

Follow the format below:

Privacy Risk: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Mitigation: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act requirements:

Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

User Consent: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Section 5: Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

5.1. What information is retained and for how long?

National and Regional Rules and Decisions – Permanent

(Records Schedule Number: DAA-0095-2018-0091)

1920	Land Management Planning	General
1920	Land Management Planning	National Forest Public Comments
1920	Land Management Planning	Regional Planning - Public Comments

EIS – Permanent
(Records Schedule Number: DAA-0095-2017-0001)

1950	Environmental Policy and Procedures	FS EIS Comments
1950	Environmental Policy and Procedures	General
1950	Environmental Policy and Procedures	Other Federal Agency Comments

EA & CE – Temporary - 15 years
(Records Schedule Number: DAA-0095-2017-0001)

1950	Environmental Policy and Procedures	Program Environmental Assessment
1950	Environmental Policy and Procedures	Project Environmental Assessment
1950	Environmental Policy and Procedures	State Environmental Impact Statements

Appeals & Litigation - Temporary – 7 years after end of fiscal year in which the case was closed
(Records Schedule Number: DAA-0095-2018-0080)

1570	Appeals and Litigation	Cases
1570	Appeals and Litigation	General
1570	Appeals and Litigation	Reports

Appeals & Litigation – Permanent
(Records Schedule Number: DAA-0095-2018-0080)

1570 Appeals and Litigation Civil court case records designated for permanent retention by court order, cases heard by the U.S. Supreme Court, cases designated as significant by the Forest Service and/or the Office of General Counsel that result in court decisions that significantly interpret statutes and regulations, cases deemed to be significant for investigative or litigation procedures or other important precedent.

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

Yes. The retention period was approved in NARA schedule DAA-0095-2017-0001, DAA-0095-2018-0091, and DAA-0095-2018-0080.

5.3. **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Retained data may become outdated or irrelevant, leading to inaccuracies in decision-making or service delivery, which can affect individuals negatively

Mitigation: Application disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and FS uses wiping tools that use NSA or DOD-approved standards to ensure secure deletion or destruction of PII (including originals, copies, and archived records.)

Section 6: Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

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

USDA NRE FS Natural Resource Manager

- First Name and Last Name

PALS shares a decision maker name (first name and last name) with NRM Forest Activity Tracking System (FACTS). FACTS uses this data to update decision makers. The information is updated and sent via encrypted backend script daily.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Unauthorized disclosure and unsecured transmission of PII.

Mitigation: Access to the application is authorized by the application Account Managers, identified by the System Owner. Data will be shared with external audiences per the System Owner's discretion and approval. Other mitigations include:

- Only authorized and authenticated users have access to the system.
- Least privilege access.
- EAuth is being used for internal users.
- Sensitive data is encrypted in transit.
- Sensitive data is encrypted at rest where possible; and
- Monitoring the security of the system on a continuous basis.

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

United States Department of Interior Environmental Protection Agency.

- First and Last Name, Email, and Phone number.

eMNEPA uses eFile to send the EIS data to e-NEPA, an EPA data sharing protocol.

6.4. **Privacy Impact Analysis**: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk:

Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

Mitigation:

Access to Application is authorized by the application Account Managers, identified by the System Owner. Other mitigations include:

- Only authorized and authenticated users have access to the system.
- Least privilege access.
- EAuth is being used for external users.
- Sensitive data is encrypted in transit;
- Sensitive data is encrypted at rest where possible; and
- Monitoring the security of the system on a continuous basis.

Section 7: Redress

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

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

There are no procedures that allow the public to gain access to eMNEPA data.

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

Members of the public cannot view data contained inside of eMNEPA. Public

comment letters stored in eMNEPA may be published to the web; these letters are viewable by the public. The public can contact the FS at any time during the NEPA process and afterwards to inquire about their information contained in eMNEPA and provide updated contact information using the project contact information provided on the web.

This is not stated in announcements. The public supplies information in order to participate in the process. Since the public can supply real, fake or no information, they can supply any contact information they choose at any time and provide updated information at any time.

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

Instructions for submitting information are provided when comments are solicited. The public can follow the instructions to submit updates to their information.

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

There is no formal communication procedure regarding information correction, nor is a formal process needed. The public can follow the instructions to submit updates to their information. FS personnel who are assigned a role on the specific project concerned can edit outdated information in eMNEPA applications.

7.5. **Privacy Impact Analysis**: Related to redress.

Follow the format below:

Privacy Risk: If the processes for individuals seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Mitigation: Individuals are required to contact a system representative to access and update any contact information. System representatives are trained at least annually.

Section 8: Auditing and Accountability

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

8.1. How is the information in the system/project/program secured?

The system protects PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

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

The system uses role-based security based on separation of duties and the least privileged access model. Roles are determined and granted by an authoritative person based on the operational and business needs of the user.

Privileged administrative users authenticate to AWS GovCloud through the AWS IAM service which includes multi-factor authentication. Authorization is enforced by AWS IAM groups. Administration of Linux servers requires SSH and a certificate. Administration of Windows servers requires RDP along with username/password.

End users authenticate for applications by first authenticating to PALS hosted at FS ACE, which implements USDA eAuthentication. The single-sign-on capabilities between PALS and eMNEPA are internally developed and managed.

8.3. How does the program review and approve information sharing requirements?

System information sharing is reviewed by the Change Control Board (CCB) following the system change management process. The CCB will seek approval from the System Owner, Authorization Official, Privacy Officer, and Assistant Chief Information Security Officer on necessary privacy paperwork to include the following: System Security and Privacy plan, Privacy Threshold Analysis, Privacy Impact Assessment, Interconnection Security Agreements, Memorandum of Understanding, and Non-Disclosure Agreement.

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

System users are required to take the Annual Information Security Awareness Training Course and Rules of Behavior. Privileged system users are required to take the Role-based security training annually. The training includes the PII security section.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 7/14/2025

USDA Privacy Analyst (On behalf of USDA's Chief Privacy Officer):

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.07.14 16:21:32 -04'00'

Signed:_______________________________________

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Signed:_______________________________________

System Owner
U.S. Department of Agriculture

Signed:_______________________________________

Mission Area Privacy Officer
U.S. Department of Agriculture

Signed:_______________________________________

ACISO
U.S. Department of Agriculture