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

Detail	Information
System/Project Name	ARS Network Information System
Program Office	Agriculture Research Service
Mission Area	REE
CSAM Number	1154
Date Submitted for Review	3/6/2025

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Joel De Armitt	Joel.dearmitt@usda.gov	202-720-5275
Information System Security Manager	Joel De Armitt	Joel.dearmitt@usda.gov	202-720-5275
System/Program Managers	Stan Kosecki	Stan.kosecki@usda.gov	202-845-5695

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 purpose of this document is to provide privacy impact analysis for the ARS Network Information System (ARSnet) at the U.S. Department of Agriculture's (USDA) Agricultural Research Service (ARS). The system resides in Beltsville, MD and provides various support services for the Agency.

Based on the results of the Privacy Threshold Analysis of the data collected, stored, and transferred through the system in support of ARS’s science mission the Privacy Impact Analysis is requiered for this system.

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 ARS Office of the Chief Information Officer (OCIO) ARS Enterprise Network provides the tools and hardware devices for help desk support, network connectivity, and upgrade of outdated software. The system provides enterprise-wide data connectivity throughout the agency, and internet access through USDA UTN. It includes three nodes in Beltsville, MD, Albany, CA and Fort Collins, CO. Additionally, the OCIO provides secondary assistance to the ARS Area Offices and Research Locations.

Enterprise Active Directory Services (including dynamic host configuration protocol DHCP), certification authority with Microsoft Active Directory Management Tools for system administrators.

Microsoft System Center Control Manager 2012 with three distribution points and Microsoft System Center Operations Manager 2007

Microsoft Hyper-V Hosts based on Windows Server 2012 technology

End user workstations based on Microsoft Windows 10 operating systems and also support Microsoft Office (including MS Word, MS Excel, MS PowerPoint, and MS Outlook), Adobe Acrobat DC client and Reader, and Juniper VPN client).

ARS maintains a small subset of servers with data storage device, containing a real time data replica, at an offsite facility in Fort Collins, CO.

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?

Code of Federal Regulations Title 5, Homeland Security Presidential Directive 12. CRIS was authorized by the Secretary of Agriculture in 1966 to document the publicly funded activities of the USDA/State agricultural and forestry research system. The system has expanded to include a number of education, extension and integrated activities. Most CRIS data is available to the public through a number of web sites. The ARIS system collects the research project data that is submitted to CRIS.

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

The system is in the process of renewing the authorization to operate and going through the assessment and authorization (formerly certification and accreditation) process. The last Authorization to Operate (ATO) was issued on June 10, 2022.

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

OPM/GOVT-1

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

N/A

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

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

Information has been acquired from employees from various functional areas (facilities, research, human resources, etc.).

2.2.1. How is the information collected?

Information is imported from USDA National Finance Center (NFC) or acquired directly from employees through various forms employees are required to fill out when onboarding.

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

The system does not use any commercial or publicly available data.

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

The information collected is no longer used nor disseminated as part of a system.

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: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Non-compliance with Regulations: Failing to accurately characterize information can lead to non-compliance with privacy laws and regulations, resulting in legal penalties and reputational damage.

Inconsistent Handling Practices: Without clear definitions and classifications, employees may handle PII inconsistently, leading to potential privacy violations.

Mitigation: By Implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

User Consent for Sensitive Data: Obtain explicit consent for the collection and processing of sensitive personal information, such as health or financial data, and ensure that users are aware of its characterization.

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?

The information is used for acquisition, employment, and research purposes. All the information collected, processed, and stored within the system is used for official USDA/ARS business only.

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.

The information collected is not used nor disseminated as part of a system.

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

Follow the format below:

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Inadequate Consent: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Mitigation: By implementing some or all the following mitigation actions, mission areas may better safeguard PII and ensure responsible use in compliance with PA requirement:

Purpose Limitation: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

Transparency: 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?

N/A

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

N/A

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

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?

The information is stored and maintained indefinitely.

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.

No approval was required since the information is retained indefinitely.

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

Follow the format below:

Privacy Risk: Privacy act risks associated with the retention of information include:

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

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

Non-compliance with Regulations: Failing to adhere to legal requirements regarding data retention periods can lead to regulatory penalties and legal liabilities.

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

Mitigation: Implementing the following mitigation actions, mission areas can ensure responsible retention of PII while complying with the PA.

Data Retention Policy: Use NARA data retention policies that outlines how long different types of PII will be retained and the rationale for those timeframes.

Regular Reviews: Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.

Secure Disposal Procedures: Establish secure methods for the disposal of personal information that is no longer needed, such as shredding paper documents or using data-wiping software for electronic files.

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?

ARSnet no longer sharing information to USDA PDSD Web Based Security Tracking System (WEBSETS), USDA National Finance Center (NFC), and USDA MD-715 for background investigation and employment purposes.

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

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?

ARSnet does not share information

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

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?

N/A

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

N/A

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

N/A

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

N/A

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

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?

Only authorized personnel are given access to the system based on need to know and least privilege principles. Access is closely monitored and logged. Physical security controls ensure only authorized individuals have access to the system components and data in storage or transit.

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

The ARS Network Information System user accounts are managed in accordance with applicable USDA account management policies and procedures. Information system users are authenticated against the Enterprise Active Directory and each user account is specific to a particular user. System, guest, anonymous, and other generic accounts, that are not specific to particular users, are prohibited. The system owner assigns responsibilities to specific parties and specific actions are defined to ensure that information system accounts are managed correctly. The process of management of the information system accounts including establishing, activating, modifying, reviewing, and locking, disabling, or deleting accounts is enforced through the use of online REE-235 and/or REE-236 forms. Before IT specialists can perform any account management action, the user's supervisor has to initiate and approve the request for account management event. The request is forwarded to ARS Account Management Team for final action. The system owner maintains records of account management actions to document that account management actions are being performed in accordance with specific procedures. At least quarterly, the same individuals who request account changes review information system accounts to ensure that continued account access is necessary. The information system automatically locks, disables, or deletes inactive accounts after 30 days of inactivity.

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

ARSnet does not share information.

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

All information system users are required to take mandatory security awareness training before being granted access to the system and at least annually thereafter.