U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

Privacy Impact Assessment

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

Agricultural Research Information System (ARIS)

Information Technology Services Division (ITSD)

REE-ARS

Date PIA submitted for review:

January 5, 2024

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	*Nicole Young*	*Nicole.young@usda.gov*	*301-504-1075*
Information System Security Manager	***Joel DeArmitt***	*Joel.dearmitt@usda.gov*	*202-720-5275*
System/Program Managers	*Stan Kosecki* *Sandra Gutierrez*	*Stan.kosecki@usda.gov* *Sandra.gutierrez@usda.gov*	*202-845-5695* *202-494-4474*

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 Agricultural Research Information System (ARIS) provides Agricultural Research Service (ARS) project research and resource management information to staff and collaborators.

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 Agricultural Research Information System (ARIS) is a key program management information system for the ARS. ARIS documents and manages multiple critical assets of ARS project research and ARS resource management including all aspects of research projects, funding levels, publications, and personnel.

The purpose of ARIS is to provide ARS project research and resource management information to mission area staff and collaborators.

Section 1.0 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?

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107

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

Authorization and Accreditation (A&A) has been initiated.

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

GOVT-1 SORN (https://www.oge.gov/web/OGE.nsf/Resources/OGE+GOVT-1+SORN+(2019))

An ARS SORN is currently in progress.

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

Information is not collected from the public.

Section 2.0 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 on 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			☐	License Plate Number
☐	Registration Number			☐	File/Case ID Number
☐	Student ID Number			☐	Federal Student Aid Number
☒	Passport number			☐	Alien Registration Number
☐	DOD ID Number			☐	DOD Benefits Number
☒	Employee Identification 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			☐	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number				
Biographical Information					
☒	Name (including nicknames)	☒	Sex	☐	Business Mailing Address (sole proprietor)

☒	Date of Birth (MM/DD/YY)	☒	Ethnicity	☐	Business Phone or Fax Number (sole proprietor)
☐	Country of Birth	☐	City or County of Birth	☐	Group/Organization Membership
☒	Citizenship	☐	Immigration Status	☐	Religion/Religious Preference
☐	Home Address	☐	Zip Code	☐	Home Phone or Fax Number
☐	Spouse Information	☐		☐	Children Information
☐	Marital Status	☒	Military Service Information	☐	Mother's Maiden Name
☒	Race	☐	Nationality	☐	Global Positioning System (GPS)/Location Data
☐	Personal e-mail address	☒	Business e-mail address	☐	Personal Financial Information (including loan information)
☒	Employment Information	☐	Alias (username/screenname)	☐	Business Financial Information (including loan information)
☒	Education Information	☐	Resume or curriculum vitae	☐	Professional/personal references
Biometrics/Distinguishing Features/Characteristics					
☐	Fingerprints	☐	Palm prints	☐	Vascular scans
☐	Retina/Iris Scans	☐	Dental Profile	☐	Scars, marks, tattoos
☐	Hair Color	☐	Eye Color	☐	Height
☐	Video recording	☐	Photos	☐	Voice/ Audio Recording
☐	DNA Sample or Profile	☐	Signatures	☐	Weight
Medical/Emergency Information					
☐	Medical/Health Information	☐	Mental Health Information	☐	Disability Information
☐	Workers' Compensation Information	☐	Patient ID Number	☐	Emergency Contact Information
Device Information					
☐	Device settings or preferences (e.g., security level, sharing options, ringtones)	☐	Cell tower records (e.g., logs, user location, time, etc.)	☐	Network communications data
Specific Information/File Types					
☐	Personnel Files	☐	Law Enforcement Information	☐	Credit History Information
☐	Health Information	☐	Academic/Professional Background Information	☐	Civil/Criminal History Information/Police Record
☐	Case files	☐	Security Clearance/Background Check	☐	Taxpayer Information/Tax Return Information

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

Non-PII information is acquired directly from employees from various functional areas (research, acquisitions, budgeting, etc.).
PII related to personnel data is imported from the USDA National Finance Center (NFC) (e.g., name, date of birth, position, etc.).

2.2.1. How is the information collected?

PII related to personnel data is imported from the USDA NFC.

Non-PII information is acquired directly from employees by manual entry by functional users and manual imports from other REE sites.

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?

Information is verified during input and checked against other records. Approval processes associated with data processing along with checks and balances built into the system ensure accurate data entry and data integrity.

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

Yes

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

Source code is managed through private repositories in Github.com; access is managed and vetted by the repository owners and reviewed annually. Privacy data, passwords or other account information are not included in the source code repositories.

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

No PII will be available through 3rd party websites/applications.

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

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.

Section 3.0 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 strictly for the unique identification of personnel. SSN is used by limited and authorized Human Resource (HR) Specialists that are responsible for collecting and reviewing personnel data from across REE and performing quality checks on the data. In performing quality checks, HR must verify employee personnel data pertaining to personnel actions including position management against data in the National Finance Center. The primary purpose of using SSN is to properly identify the employee. Many employees have similar names, and the use of SSN enables HR to identify the correct employee for purposes of verifying the employee regarding personnel action. The information is used only by offices and employees who have a need for the information in the performance of their official duties.

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.

ARIS does not use any type of tools to analyze PII data. No PII data is "produced". PII data is not manipulated.

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 safeguard PII better 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.

privilege principles. Authentication is provided by USDA LincPass access to privileged users only and data access is limited to a need-to-know basis controlled by application security levels and roles.

Section 4.0 Notice

The following questions are directed at providing 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.

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

ARIS does not collect privacy information. The privacy data is imported from NFC.

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

All PII data is maintained solely for the unique identification of personnel and is accessible only to authorized users with a need to know in the performance of their official duties.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

Privacy Risk: **Privacy Act risks associated with notices include:**

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

Ambiguity: 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.

Non-compliance with Regulations: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

Mitigation: The system displays a login banner when entering the system and users must acknowledge and consent to all information on the computer system being intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes. All PII data is maintained solely for the unique identification of personnel and is accessible only to authorized users with a need to know in the performance of their official duties.

Section 5.0 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?

PII information is stored and maintained based on federal government data retention policies and NARA general records schedule 4.2 or ARS NARA approved retention schedule.

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.

NARA general records schedule 4.2

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.

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 outline 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 6.0 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?

ARIS does not transmit or share any PII data with any other internal USDA organization.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Risk of sharing PII data with internal USDA organizations.

Mitigation: This risk is mitigated as ARIS does not share PII data with any other organizations. Only specific non-PII data elements are shared via manual processes that are controlled and data reviewed for correctness.

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?

ARIS does not share privacy data with external organizations.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.
Follow the format below:

Privacy Risk: Risk of sharing PII data with external organizations.

Mitigation: This risk is mitigated as ARIS does not share privacy information with external organizations.

Section 7.0 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?

Individuals should contact the original source (Human Resources/NFC) to gain access to their information or to request changes.

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

Individuals should contact the original source (Human Resources/NFC) to request changes to their information.

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

Individuals should contact the original source (Human Resources/NFC) to gain access to their information or to request changes.

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

Employees have formal lines of communication with their human resources representative and can request access to and correct their information when necessary.

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk: Inaccurate or erroneous information

Mitigation: Employees have access to their information at the original source (Human Resources/NFC), and can request change/correction of their information, when necessary, as part of regular Human Resources activities. There is no identified risk.

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?

PII data is encrypted at rest and in transit. In addition, access to the system requires multifactor authentication into the USDA network and data access is limited to "need to know" basis controlled by application security levels and roles.

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

USDA user accounts are managed in accordance with applicable USDA and ARS account management policies and procedures. Information system users are authenticated using USDA multifactor authentication 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 initiates and approves the request for account management event. The request is forwarded to IT specialists for final action. The system owner or their delegate maintains records of account management actions to document that account management actions are being performed in accordance with specific procedures. System account administrators regularly review information system accounts to ensure that continued account access is necessary. The information system automatically locks, disables, or deletes inactive accounts after 60 days of inactivity through OCIO CEC user account procedures. User management procedures are documented in standard operating procedure manual.

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

The REE governance process includes applicable legal, policy, privacy, and ethical review and approval of information sharing agreements, Memoranda of Understanding/Agreement, and ARIS system connects at the appropriate level for the proposed sharing/connection.

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.