Privacy Impact Assessment

Agricultural Research Service (ARS) Administrative and Financial Management (AFM) Customer Service Portal (CSP)

Policy, E-Government and Fair Information Practices

- Version: 4.0
- Date: August 5, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

ARS AFMCSP

5 August 2020

Contact Point

Masiel Morales
USDA/ARS/AFM/DAAAFM
209-373-8267

Reviewing Official

Nicole O. Young
Privacy Officer - ARS
United States Department of Agriculture
301-504-1075

Abstract

The Agricultural Research Information System (ARIS) is the U.S. Department of Agriculture's (USDA) computer-based documentation and reporting system for ongoing and recently completed projects in agriculture, food and nutrition, and forestry research.

Based on the Privacy Threshold Analysis results the Privacy Impact Analysis is recommended for this system.

This Privacy Impact Assessment (PIA) is for the USDA, Agriculture Research Service Administrative and Financial Management Customer Service Portal. The ARS AFMCSP system provides a web-based tool that enables ARS personnel to submit, assign, track, and close requests through the various modules contained within the AFMCSP application. This PIA is being conducted to determine the potential impact of the data which is collected via ARS AFMCSP.

Overview

ARS AFMCSP consists of a set of secure web-based interfaces on the SalesForce platform, which includes the modules listed below and supports ticketing requests.

In short, ARS AFMCSP:

- Provides a web-based tool that serves as a one-stop-shop ticketing request tracking system for AFM administrative functions including Human Resources (HR), Information Technology (IT), and Space Management (SM), among others.
- Modules include: Budget, Engineering, IT Requests, Personal Property, Real Property, Safety and Health, Travel, Space Management, User Management, Acquisitions, Agreements, Human Resources, Custom Dashboards, Partner Agencies, Data Calls, Integrated Project Management, Acquisitions Tracking System, and Portal Issues Management.
- Submitted tickets are tracked from opening through fulfillment and closure.

This PIA is being created for the ARS AFMCSP application which is a cloud provided solution.

Section 1.0 Characterization of the Information

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

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

The AFMCSP application collects privacy information about ARS employees and contractors, as well as Foreign and US Nationals for future employment who voluntarily discloses the information on a job application or travel application. The PII collected is:

- Name
- Date of birth
- Address information
- Social Security Number (SSN)
- Biometric data
- Criminal history
- Employment history
- Miscellaneous identification numbers
- Photographic images/identifying characteristics
- Handwriting or image of the signature

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

Information is acquired directly from employees from various functional areas (facilities, research, human resources, etc.) Additional employee records are manually imported from USDA National Finance Center (NFC) (e.g. name, date of birth, position, retirement, service comp date).

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

The information is collected, processed, and maintained for background investigations, Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors (HSPD12), employment purposes, court settlements, and in order to support the agency's mission (Agricultural Research) and facilitate tracking cost expenditures.

1.4 How is the information collected?

The information is collected manually and electronically.

1.5 How will the information be checked for accuracy?

On recruitment and other related documents, the individuals are given the opportunity to review the information and correct as necessary. On existing records, Human Resources employee representatives provide employees with procedures for correcting their information if needed.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Code of Federal Regulations Title 5, HSPD12. Current Research Information System (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.

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

The information collected when obtained as a whole could identify individuals and their activities with regards to AFMCSP activities and employment history. This information is protected through various levels of security and policy. The system itself is protected by role based access layers and positive identification techniques to ensure that only people authorized to view information about others can do so.

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The principle purpose of collecting data from an individual is to collect information related to employment opportunities. The information is collected, processed, and maintained for background investigations, HSPD12, employment purposes, court settlements, and in order to support the agency's mission (Agricultural Research) and facilitate tracking cost expenditures. All the information collected, processed, and stored within the system is used for official USDA/ARS business only.

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

Not Applicable – there are no special tools in use and no data will be produced by analysis

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

Not Applicable – the system does not use commercially or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The information is protected through various levels of security and policy. The system itself is protected by role based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so.

Section 3.0 Retention

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

3.1 How long is information retained?

The HR records are retained while the employment lasts and 65 years thereafter. ARIS Application records are retained for at least 10 years. Electronic copies of all records mentioned in this document are stored online in database and on disk arrays, and offline on backup media. The system IT personnel ensures adequate storage is provided. Some HR records are retained indefinitely as defined "permanent value" by NARA. https://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/chapter-4.html.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes. NI-310-03-1 and GRS 1, item 1.

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

Given the length of time data is retained within the system, the agency recognizes the risk of inadvertent privacy data disclosure. The risk is mitigated through a series of security measures built into the cloud provider system that is FedRAMP certified– starting with the physical security of the system, restricted access, all the way to logical security controls that carefully control access to the information.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

ARS does not share this data with any internal organizations – all access is maintained within the Human Resources and Leadership of ARS.

4.2 How is the information transmitted or disclosed?

Not applicable. ARS does not share this data with any internal organizations.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Not applicable. ARS does not share this data with any internal organizations.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

The information is not shared with any external organization.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

Not Applicable – the information is not shared with any external organization.

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

Not Applicable – the information is not shared outside the Department.

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

Not Applicable – the information is not shared outside the Department.

Section 6.0 Notice

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

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

GOVT-1: General Personnel Records SORN

https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf

6.2 Was notice provided to the individual prior to collection of information?

Yes. USDA requires that agencies: inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information;

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

No, information must be entered as a condition of onboarding employees into ARS. All information must be provided as a requirement of employment with ARS.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

No. The information is explicitly for use by the ARS Human Resources and leadership team. The individuals do not have the right to consent to particular uses of the information. Information entered is used throughout the ARS onboarding process

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

Notice is provided to the individuals of the collection of data as part of the ARS onboarding process, and is required for employment with ARS. There are no risks to be mitigated, as individuals are aware of the collection process

Section 7.0 Access, Redress and Correction

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

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

Employees have access to their HR information through their human resources employee representative or OPM Electronic Official Personnel Folder (EOPF).

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

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

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

Human resources employee representatives provide employees with procedures for correcting their information.

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

Not Applicable – formal redress is provided.

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

Not Applicable - there are no privacy risks associated with the redress available to individuals.

Section 8.0 Technical Access and Security

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

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

The ARIS information system user accounts are managed in accordance with applicable USDA and ARS account management policies and procedures. The following applies to all information system components (applications and database): 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 area program analyst or budget fiscal officer has to initiate the request for account management event. The request is approved by the functional sponsor and forwarded to IT specialists 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 monthly, the same individuals who request account changes review information system accounts to ensure that continued account access is necessary.

The information system automatically locks and disables inactive accounts after 60 days of inactivity.

8.2 Will Department contractors have access to the system?

Yes, there are contractors within Human Resources that will have access to the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

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

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

Yes, this was completed on 03/22/2018

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

All users are required to have an individual user account to access the application. Deletion of data is audited within the application, and extraction cannot be performed except through authorized user access to the portal itself.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

ARS institutes the best industry practices for safeguarding PII and FIPS 199. The information is protected through various levels of security and policy. The system itself is protected by role based access layers and positive identification techniques to ensure that only people authorized to view and act upon information about others can do so.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 What type of project is the program or system?

ARS AFMCSP is a web based information system on a cloud based system.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

The system does not utilize any technologies that would raise privacy concerns.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes.

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

Not Applicable – There are no third party websites in use with the application.

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

Not Applicable – PII does not cross third party websites.

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

Not Applicable – PII does not cross third party websites.

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

Not Applicable – PII does not cross third party websites.

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

Not Applicable – PII does not cross third party websites.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

Not Applicable – PII does not cross third party websites.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

Not Applicable – PII does not cross third party websites.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

Not Applicable – PII does not cross third party websites.

10.10 Does the system use web measurement and customization technology?

Not Applicable – PII does not cross third party websites.

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

Not Applicable – PII does not cross third party websites.

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

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

Not Applicable – PII does not cross third party websites.

Responsible Officials

Masiel Morales, Agricultural Research Service
(ARS) United States Department of Agriculture

Approval Signature

NICOLE YOUNG Digitally signed by NICOLE YOUNG
Date: 2020.08.19 12:56:12 -04'00'

Nicole O. Young
Privacy Officer
Agricultural Research Service
United States Department of Agriculture