Privacy Impact Assessment
ICAM Shared Services

Policy, E-Government and Fair Information Practices

- Version: 1.8
- Date: July 2021
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA
United States Department of Agriculture

Privacy Impact Assessment

ICAM Shared Services

July 2021

Contact Point

Shari Arduini
CEC/IOD/IASB
970-295-5128

Reviewing Official

Nancy Herbert, ISSPM
CEC
816-926-3826

Abstract

This Privacy Impact Assessment is for the Identity, Credential, and Access Management Shared Services (ICAMSS) encompassing eAuthentication (eAuth), Enterprise Identity Management Service (EIMS), Application Programming Interface Security – API Security (API Sec), Privilege Management (PRIVMGT) and enterprise Public Key Infrastructure (ePKI).

ICAMSS provides an integrated set of tools to manage USDA users, their respective roles, and their access privileges in an automated manner. The ICAMSS solution centralizes and automates identity and access control related processes to help reduce costs, manage IT security risk, enable new business opportunities, and improve compliance. The solution supports the identity lifecycle across every IT environment – from the Web to the mainframe. ICAMSS integrates with existing USDA applications and systems, such as HR data sources and enterprise applications (e.g. WebTA, ePACS, Enterprise Active Directory, etc). ICAMSS aggregates data from these systems into a single master user record. At the core of ICAMSS are CA Technologies, Radiant Logic, SailPoint, and CyberArk products that are comprised of a variety of modules. With the addition of Continuous Diagnostics & Mitigation (CDM) program concepts within ICAMSS, the system is focused on "Who is on the Network" and has components to arrive at that answer through: Manage Trust in People Granted Access (TRUST); Manage and Security Related Behavior (BEHAVE). Those modules represent the functionality that the Department requires to implement the ICAMSS architecture needed to resolve many of the persistent access management issues.

ICAMSS provides the ability to centrally manage person and role data and provide self-service functionality through portals. ICAM Shared Services includes a Rules Engine allowing for dynamic processing of person data to define roles and access rights in an automated manner, while the Workflow Engine facilitates the routing of information, tasks, and events, such as access requests and approval processes. The Auditing & Reporting and Monitoring components are used to show when an identity was created and by whom; what a person can access; what a person did to access; when their status changed; who initiated it; etc. Management of each of these components is provided via Administration functions, which allow configuration of the system, including role and access administration, use of configuration files, scripts, API calls, etc.

The implementation of Online Identity Proofing service validates customer's identity to authorize identity assurance level (IAL) 2 accounts based on NIST SP 800-63. A third-party Credit Bureau provides the capability to evaluate users based on using a dynamic Knowledge Based Authentication (KBA) designed to identify a user through a randomly generated set of questions maintained by the Credit Bureau. Depending on the success of those questions, those customers receive a risk score associated to the confidence level that this individual is who they say they are. The Out Of Wallet (OOW) questions, can be but are not limited to, Driver's License, Social Security, Credit Card Numbers and/or Account Numbers verified. Depending on the risk score the vetted process of the user's evaluation will determine the IAL 2 authorization.

Overview

The major aspects of ICAM Shared Services include:

- Major Application (MA) and High Value Asset (HVA).
- Comprehensive solution that provides a single point of control to manage across the entire organization including employees, contractors, visitors, temps, appointees,and partners.
- Handles and verifies standard HR information.
- Shares standard HR information with USDA agencies.
- Designed as a security front end to provide authentication and authorization to web-based applications. The data stored within ICAMSS is used to determine authentication and application access.
- Collects personal information to verify the identity of the user both in person and through Identity Proofing practices based on NIST 800-63.
- Provides a single sign on capability as a front end to USDA applications.
- Discloses information based on the System of Record Notice (SORN).
- ICAMSS has no subsystems.

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 following personal data is handled by ICAM Shared Services:

Account Creation Date	CRED Type	Home Zip Code Email Address
Account Identifier	Date Account Status Initiated	Last Name
Account Identifier	Date Assigned Behave Expires	Middle Name
Account Status	Date Behave Create/Assigned	Phone
Account Status Grace Period	Date CRED Issued/Tracked	Preferred First Name
Account Type	Date CRED Status Initiated	PRIV Description
Behave Description	Date Issued CRED Expires	PRIV Identifier
Behave Identifier	Date of Birth	PRIV Status
Behave Name	Date Trust Expires	PRIV Type
Behave Status	Date Trust Frist Tracked	Social Security Number
Behave Type	Date Trust Last Reviewed	Suffix Name
Citizenship Home Address	Date Trust Status Initiated	Trust Description
Country of Birth	Ethnicity Mobile Phone	Trust Identifier

CRED Description	First Name	Trust Name
CRED Identifier	Gender	Trust Review Grace Period
CRED Identifier	Home City	Trust Status
CRED Status	Home State	UserID

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

The sources of ICAMSS data are Human Resources Person Model, Web based Security Entry and Tracking System (WebSETS), AgLearn, and USAccess. Some data is also supplied by external customers of USDA during the creation of an eAuth account. Personal information for USDA employees, contractors, affiliates, interns, fellows, and volunteers is supplied to ICAMSS via human resources.

1.3 Why is the information being collected, used, disseminated, ormaintained?

The information is collected to provide accurate personnel information to the agencies they work with. The data is used to determine user privileges within enterprise and agency systems. The data provides the capability to determine accessibility for web access control.

1.4 How is the information collected?

Data is transferred electronically (encrypted) from the sources named in question 1.2, along with self-registration data supplied by the user to access USDA web applications.

1.5 How will the information be checked for accuracy?

Data received from the HR systems is considered correct and authoritative; however, Social Security Number and Date of Birth values are checked to ensure they are within an acceptablerange. This validation will trap obvious errors and prevent some invalid data from being transmitted to other systems. External USDA customers must have their information checked by a Local Registration Authority (LRA) or the online identity proofing during the account registration process.

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

USDA shall comply with all federal laws, rules, regulations, and decisions applicable to the credit bureau's provision of the credit bureau data and the Services pursuant to this Agreement.NIST SP 800-144 states, "Organizations are ultimately accountable for the security and privacyof data."

A. Gramm-Leach-Bliley Act. All parties shall implement and maintain a comprehensive information security program written in one or more readily
accessible parts and that contains administrative, technical, and physical safeguards that are appropriate to Client's size and complexity, the nature and scope of its activities, and the sensitivity of the information. Such safeguards shall include the elements set forth in 16 C.F.R. § 314.4 and shall be reasonablydesigned to (i) ensure the security and confidentiality of the information, (ii) protect against any anticipated threats or hazards to the

security or integrity of such information, and (iii) protect against unauthorized access to or use of suchinformation that could result in substantial harm or inconvenience to any consumer.

B. NIST 800-63 outlines the specific requirements for Online Identity Proofingboth remotely and in person. USDA follows those guidelines to provide a service to agencies on the use of the appropriate assurance level.
C. E-Government Act of 2002 (Public Law 107-347) which defines Identifiable Form and addresses the exchange of government informationwith external/public entities.
D. The information exchanged is regulated by an Interconnection SecurityAgreement (ISA).

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

The ICAMSS systems are in a restricted environment. The database is only accessible by a few system administrators. Sensitive data at rest is encrypted. Two methods comprise access.

1. All administrators are required to use PIV Card to access all system components. An administrator must have their one user account to access USDA web application.
2. All external users are required to use their eAuth user account and password to be authorized to view their own specific data.

The ICAM data repository uses certificate-based authentication with limited users. The environment is highly controlled. End user's data access is controlled by roles, and access is very limited which also requires a PIV Card for authorization. All transactions are logged. Connectivity to the credit bureau services takes risk in account based on NIST 800-95, *Guide to Secure Web Services,* and NIST 800-63*, Digital Identity Guidelines.*

Section 2.0 Uses of the Information

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

2.1 Describe all the uses of information.

The information is collected to provide accurate personnel information to the agencies they work for. The data is also used to determine user privileges within the enterprise system.

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

ICAM identity management systems provide the ability to centrally manage person and role data and provide self-service functionality through portals. CA Technologies, SailPoint, CyberArk, Radiant Logic tools are used for management of identities in agency/endpoint

accounts and data stores. SQL and LDAP tools may be used by a restricted group of systems analysts to troubleshoot issues.

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

Yes, commercial data or publicly available data is used. The online identity proofing process uses a third-party Credit Bureau which provides the capability to evaluate users based on usinga dynamic Knowledge Based Authentication (KBA) design to identity a user through a randomly generated set of questions maintained by the Credit Bureau.

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

Role Based Access Control (RBAC) is used to limit who has access to data.

Section 3.0 Retention

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

3.1 How long is information retained?

The data is kept in accordance with the National Archives and Records Administration based on the last time the user accessed the service.

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

The retention period follows the National Archives and Records Administration based on the last time the issuer accessed the service.

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

Data in this system is kept only as long as necessary. Sensitive PII data is encrypted at rest. Only a limited amount of administrators have access and their access is review monthly and quarterly.

Section 4.0 Internal Sharing and Disclosure

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

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

Data is received from EmpowHR, NEIS, Payroll Personnel, and data is provided to all connected USDA agencies.

4.2 How is the information transmitted or disclosed?

The EIMS, a component of ICAM, is used to share data. Data is transmitted via encrypted connections to USDA Agency servers. Information queried by the National Credit Bureau's repository follows Gramm-Leach Bliley Act, Privacy Act of 1974, NIST 800-95, and NIST 800-63 requirements to provide Confidentiality, Integrity and Availability of the information.

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

Role Based Access Control (RBAC) is used to limit who has access to data. Connections areencrypted.

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, whatinformation is shared, and for what purpose?

Data is shared with the General Services Administration (GSA) via the HSPD 12 PIV card provisioning system.

For online identity proofing the Social Security Number is shared via a web service between ICAMSS and a national credit bureau in accordance with the Gramm-Leach-Bliley Act. Mutual Authentication and Certificates are created to encrypt the data between both entities. This allows the national credit bureau to conduct analysis with the user to verify the identity of the individual in accordance with NIST 800-63 requirements for IAL2 accounts. The Social Security Number is not stored in ICAMSS system. This is an inquiry on already existing data available to the national credit bureau in accordance with Gramm- Leach- Bliley Act.

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 theprogram or system is allowed to share the personally identifiableinformation outside of USDA.

The data shared with GSA and the national credit bureau is compatible with the original plan of this system. A SORN is in place to cover the collection of data for ICAM Shared Services, see section 6.1.

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

Certificate based message level encryption is used. Mutual Authentication is also utilized to ensure that both hosts receive confirmation before transmitting. The tunnels are encrypted to protect eavesdropping and session hijacking. An Interconnection Security Agreement (ISA) is established to ensure that all compliance needs are met.

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

	Message Alteration	Loss of Confidentiality	Falsified Message	Man in the Middle	Principle Spoofing	Forged Claims	Replay of Message Parts	Replay of Message
XML Encryption		X		X	X	X	X	
XML Signature	X		X		X	X	X	X
WS-Security Tokens			X		X	X		
WS-Addressing								X
SSL/TLS	X	X	X*	X	X*	X*	X	
SSL/TLS with Client Certificates	X	X	X	X	X	X	X	
HTTP Authentication			X		X	X		

The table shows the risks and the mitigating technologies that resolves those areas. To further enhance these controls, exportable private keys are stored in a software key store with password protection to further control these methods. The system is placed in a server cluster to increase availability.

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 provideSORN name and URL?

Yes, see USDA/OCIO-2 eAuthentication
https://www.federalregister.gov/documents/2017/01/26/2017-01767/privacy-act-of-1974-revised- system-of-records#page-8504

The SORN will be updated n FY21 to reflect the system name change from eAuthentication Application to ICAM Shared Services.

6.2 Was notice provided to the individual prior to collectionof information?

Individuals supply this information to Human Resources based on their function within the USDA. They are told this information will be used for physical and electronic access. External customers are told what the collected information will be used for and the system utilizes the standard notification in accordance with USDA.

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

6.4 Providing information can be refused, but the data collected is a condition of employment withUSDA. Yes, external customers can refuse to provide their information and not create aneAuth account.Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Providing information can be refused, but the data collected is a condition of employment with USDA. External customers can refuse to provide their information and not create an eAuth account.

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

Individuals are made aware of what the information will be used for when it is collected by Human Resources. External customers are made aware through disclaimers when an account is going to be created.

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?

Individuals can access their own profile information that is stored in the ICAMSS user store.

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

Individuals can access their own profile information that is stored in the ICAMSS user store.

7.3 How are individuals notified of the procedures for correcting theirinformation?

Individuals are told by their supervisor or the Help Desk of the ability to go to HR to examine and correct their personnel file and/or their own profile information that is stored in the ICAMSS user store.

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

Formal redress does exist as stated above.

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

Data sent to ICAM from HR is only accessible by each individual. If there is any question about the accuracy of the data, the individual is instructed to contact HR to correct.

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 accessthe system and are they documented?

The system contains automated workflows that can be customized to automatically provide a minimum level of access. This access is based on an individual's relationship with the USDA (i.e., having an HR record in the USDA HR system). Other levels of access can be granted with supervisor approval or approval from a higher-level authority. All access transactions, including approvals, additions, or removals of access are fully logged by the system. Administrators having access is documented and evaluated based on a 30-day window and a quarterly review.

8.2 Will Department contractors have access to the system?

Yes, contractors and other non-employees have access. Refer to section 8.1.

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

The USDA OCIO mandates Privacy training annually through AgLearn.

8.4 Has Certification & Accreditation been completed for the system orsystems supporting the program?

Yes.

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

Automated periodic account reviews are conducted 30 days and quarterly. Agency supervisors must certify that account access requirements are being met by all users. ICAM also certifies required access and logs the certification. The ICAM system is subject to all USDA Department level requirements for hosting, data management, data transmission, and security best practices. ICAM is subject to A-123 and other compliance audit processes. A disclaimer for OIDP actions is presented to the user, notifying the user of the use of the PII information and the need for the process to occur for online identity proofing. SSN is masked to protect the user's PII.

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

Automated periodic account reviews are conducted both monthly and quarterly. Agency supervisors must certify that account access requirements are being met by all users. ICAM also certifies required access and logs the certification. The ICAMSS system is subject to all USDA Department level requirements for hosting, data management, data transmission, and security best practices. The ICAMSS is subject to A-123 and other compliance audit processes.

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?

ICAMSS is a Major Application (MA) and a High Value Asset (HVA).

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

None of the technology used presents any unusual privacy issues.

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 ofWeb 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 websitesand/or applications?

The purpose provides Online Identity Proofing to evaluate the individuals for a IAL 2 account under NIST SP 800-63.

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

The social security number, date of birth, phone number, and name will be provided to a national credit bureau under the Gramm Leach Bliley Act (GLBA) – Financial Services Modernization Act of 1999.

10.4 How will the PII that becomes available through the agency's use of3rd party websites and/or applications be used?

The purpose provides Online Identity Proofing to evaluate the individuals for an IAL 2 account under NIST SP 800-63.

10.5 How will the PII that becomes available through the agency's use of3rd party websites and/or applications be maintained and secured?

The application uses SSL encryption and mutual authentication to protect PII information.

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

The social security number is not stored on any USDA systems. The National Credit Bureau must follow the GLBA in protecting the existing information store on individuals. The system does allow the user to decline and utilize an alternative method for identity proofing an individual.

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

No individuals have access to social security number information. The system will query existing information from the credit bureau. This is a system to system connection.

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

The system queries existing PII data provided by the credit bureau. There is no other information shared outside of the relationship.

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

Yes, the System of Records Notice is available.

10.10 Does the system use web measurement and customization technology?

N/A

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

N/A

10.11 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.

Technically – the connection between the existing system and the national credit bureau is SSL encrypted and mutual authentication, which provides protective measures.

PII data was required by NIST 800-63 to identity proof individuals – the utilization of the credit bureaus provided an approach that was protected by the GLBA. USDA does not store the social security number.

Responsible Officials

PHILLIP RENDINA

Digitally signed by PHILLIP RENDINA
Date: 2021.06.21 12:55:20 -05'00'

Phillip Rendina
OCIO-CEC-IOD, Director
United States Department of Agriculture

Date

Agency Approval Signature

NANCY HERBERT

Digitally signed by NANCY HERBERT
Date: 2021.06.21 12:28:01 -05'00'

Nancy Herbert
OCIO-CEC-GSD-SCSB, ISSPM
United States Department of Agriculture

Date