Office of the Chief Information Officer
U.S. DEPARTMENT OF AGRICULTURE

USDA Privacy Impact Assessment

Fiscal Year 2025

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	Enterprise Active Directory (EAD)
Program Office	OCIO
Mission Area	CEC
CSAM Number	1990
Date Submitted for Review	8/7/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Hugh Woolard	816-926-3446
Information System Security Manager	Robert Lee	910-431-8634
System/Program Managers	Innocent Lau	314-457-4614

Abstract

This Privacy Impact Assessment (PIA) supports the Client Technology Services (CEC) Enterprise Active Directory (EAD) Major Application information system. The CEC EAD provides a USDA-wide directory service to implement a common directory structure and common security group-policy-objects (GPOs). This PIA is being completed due to a Privacy Threshold Analysis (PTA) that indicated a PIA was required for the EAD system to meet Federal privacy compliance requirements.

Overview

The Department of Agriculture (USDA) has implemented the Microsoft developed Active Directory (AD) application. 'Active Directory' is a directory service, included in Windows Server operating systems that are used for managing network objects in Windows domain networks. EAD is integrated with existing Department-wide applications and services via the Microsoft Active Directory Federation Services (ADFS). ADFS is a claims-based federation service (authentication) deployed in EAD to support Single Sign-On-enabled web applications across various domains. The EAD information system enables USDA to centralize management of network resources, applications and users. User accounts are created and stored as objects in Active Directory (AD) Domain Services. Each user that accesses resources in the Windows domain must have a user-access-account in the Active Directory service. The AD account is used to identify and authenticate the specific user so that the specific user may use a specific network-resource.

Section 1: Authorities and Other Requirements

These questions identify all statutory and regulatory authorities for operating the project, application, or system, including the authority for collection, which SORN applies, if an ATO has been completed, and if there is Paperwork Reduction Act coverage:

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

- Department Regulation, DR 3515-002
- Government Paperwork Elimination Act (GPEA, Pub. L. 105–277) of 1998
- Freedom to E-File Act (Pub. L. 106–222) of 2000
- Electronic Signatures in Global and National Commerce Act (E–SIGN, Pub. L. 106–229) of 2000

Has Authorization and Accreditation (A&A) been completed for the project, application, or system?

Yes, approved 8/21/2024. The EAD system is in Continuous Monitoring of the USDA RMF.

Which System of Records Notices (SORNs) apply to the information?

Yes. SORN: USDA/OCIO-2, eAuthentication – USDA.OCIO-2

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

No

Section 2: Information Characterization

These questions define the scope of the information requested and collected, as well as the reasons for its collection as part of the project, application, or system being developed:

What information is collected, used, disseminated, or maintained in the project, application, or system? 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.

Biographical Information:

- Name (including nicknames)
- Employment information
- Business phone or fax number (sole proprietor)
- Alias (username or screenname)

What are the sources of the information in the project, application, or system?

The source of the information is provided by individual Agency Provisioning Policies and Procedures. These may include both automated and manual data entry components. The CEC supported agencies utilize a System Access Authorization Request (SAAR) process initiated by the supervisor\manager. The Forest Service utilizes an automated provisioning system provided by the Enterprise Entitlements Management Service (EEMS) utilizing data from HR and contracting systems. Additionally, some data attributes\fields are synchronized from the Enterprise Entitlements Management Service (EEMS) to each and every user object.

How is the information collected?

This information is used to provision and/or modify Active Directory (AD) user access-accounts and e-mail address. The information is included in the listing (directory service) of user access accounts. A user-account is used to enable a human user to log on and access end-point devices and subsequently access other resources on the USDA-Managed-Enterprise network and from cloud services.

Does the project, application, or system use information from commercial sources or publicly available data? If so, explain why it is used.

No commercial or publicly available data is used as input to the EAD system.

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

Information is supplied by the authorized agency personnel requesting that a user account be added, modified or deleted in EAD. The Microsoft Active Directory management module performs data validation in so far as to check the data that is input is in the proper format for use within Active Directory, e.g. a user access account logon name cannot contain a '. The data accuracy is verified by the agency account operators using established policies and procedures. Data fields synchronized from the EEMS system will maintain consistent accuracy with the authoritative source.

Does the project, application, or system use third-party websites?

Yes

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

N/A

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

N/A

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

Privacy Risk

- **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.

Mitigation

- **Data Classification Policy**: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.
- The Active Directory database is a Lightweight Directory Access Protocol (LDAP) system requiring specialized tools and viewers to access both visible and normally hidden data sets. Compensating controls to limit access to the tools for users and systems from both inside and outside the USDA corporate network are in place. The USDA Privacy Office does not acknowledge a 'Rolodex Exception'. The USDA Privacy Office mandates the use of the Privacy Overlay in any system where PII is identified.

Section 3: Information Uses

These questions delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated and/or maintained will support the project, application, or system's business purpose.

The information is used to generate a (human) user's access account. That user account is then used to authenticate to the Network and access network resources. The information is also used to populate business contact information in the GAL.

Custom scripts are used to gather and analyze access metrics, by User-access-account name. This information is processed and formatted to produce access control reports e.g. last logon date and time, last modification to account.

Does the project, application, or system 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.

No commercial or publicly available data is used as input to the EAD system.

Privacy Impact Analysis: Related to uses of the information. Follow this format:

Privacy Risk

- **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.

Mitigation

- Implement access controls to restrict who can use personal information and for what purposes, ensuring that only authorized personnel have access to sensitive data.

Section 4: Notice

These questions are intended to provide 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.

How does the project, application, or system provide notice to individuals prior to collection?

Upon employment/contract, Individuals supply PII data elements to Human Resources systems based on their Role within the USDA. They are told this information will be used for physical and electronic access.

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

No. Providing information to be used in the account provisioning process is a condition of employment.

Privacy Impact Analysis: Related to notice.

Privacy Risk

- **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.

Mitigation

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

Section 5: Data Retention

These questions outline how long information will be retained after the initial collection.

What information is retained and for how long?

Each specific User Access Account/GAL contact information is maintained for the duration of time that the individual is a federal employee, contractor, or other partner requiring access to the Organization network resources. User Access Accounts are disabled utilizing the respective agency provisioning policy and procedures. Accounts are automatically disabled after 30 days of inactivity by agency automation. User Access Accounts are deleted by the respective Account Management Standard Operating Procedures.

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

The retention period for user-access-accounts is approved by the Component System Owner, in compliance with the Department RMF Guidance supporting NIST 800-53 rev4 security controls implementation.

Privacy Impact Analysis: Related to data retention.

Privacy Risk

- The retention period for user-access-accounts is a function of business need. Risks associated with the length of time data is retained include phishing and social engineering (e.g. Business E-mail Compromise (BEC). These risks are mitigated through the use of Annual Security Awareness Training, monthly Security Bulletins, scheduled Access Monitoring reports and a rigorous Account Management Standard Operating Process as well as a PIV technical mandatory.

Mitigation

- Use NARA data retention policies that outline how long different types of PII will be retained and the rationale for those timeframes.

Section 6: Information Sharing

These questions define the content, scope, and authority for information sharing.

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

The Microsoft Exchange-component-system of the CEC Microsoft – Office 365 Multi-Tenant & Supporting Services (O365MT) system and the Microsoft Azure Government Community Cloud (GCC) accesses the Global Address List in EAD. Individual users within each EAD-Member-Organization can view the Global Address List (GAL). The GAL contains business contact information. Contact is used for distribution list and email purposes.

The administrative management agent for Active Directory global address list (GAL) is preconfigured with rules that synchronize data in Active Directory forests. These forests are enabled for Microsoft Exchange Server and Microsoft Azure AD Connect to synchronize user objects and attributes across forests.

Privacy Impact Analysis: Related to internal information sharing and disclosure.

Privacy Risk

- **Unauthorized Access**: Employees may access PII without proper clearance, leading to potential misuse.
- **Data Breaches**: Internal systems can be vulnerable to breaches, compromising PII.

Mitigation

- Develop a clear policy outlining the conditions under which PII can be shared externally, including legal and compliance requirements (ex.: Computer Matching Agreements, SORNs, Business Agreements).

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

User Access Accounts exist in EAD. User Access Accounts are synchronized to the Microsoft Azure GCC environment, with authentication being provided by EAD ADFS.

The synchronization of the user attributes is required for routine use of email, SharePoint and office products, and to link that usage to employment or continued involvement with USDA. SORN: USDA/OCIO-2, eAuthentication – USDA.OCIO-2.

The data is synchronized utilizing secure encrypted channels across approved ENS MPS and Microsoft networks. The Microsoft Azure AD Connect product is utilized to limit scope and attributes for synchronization.

Privacy Impact Analysis: Related to external information sharing and disclosure.

Privacy Risk

- **Unauthorized Access**: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.
- **Data Breaches**: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.
- The data risk is to both GAL, rolodex and unique identifier attributes. This data is protected by compensating controls found both in the EAD FISMA High and Moderate control implementations but also by the Microsoft FEDRAMP.

Mitigation

- Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.

Section 7: Redress

These questions address the individual's ability to ensure the accuracy of the information collected about him or her.

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

For the User Access Account: An individual does not have access to the key data elements used for identifying and authenticating to the organizational network environment [e.g. User Account name]. An Individual may access their business contact information (GAL) by going into Outlook, select the "Search address book" icon then enter their name with last name first. Once located, the user must double click on his/her directory listing, and their detailed information will appear.

What are the procedures for correcting inaccurate or erroneous information?

An individual user may update certain data elements of their contact information by utilizing the AD Self-Service website or through a respective agency account management request. The user access account logon name and email address are provisioned by EAD per respective agency Account Management naming convention procedures following EAD Object Naming Standards.

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

Individuals are told by their supervisor or agency Help Desk the agency specific procedures required to modify User Access Accounts and GAL data.

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

N/A

Privacy Impact Analysis: Related to redress.

Privacy Risk

- **Inadequate Processes**: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.
- **Lack of Transparency**: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Mitigation

- User Access Accounts are only accessible by Domain Administrators and User Account Administrators. The GAL is viewable within the EAD network. Redress procedures are in place.
- Establish feedback channels for individuals to provide insights into the redress process, helping to improve the system continuously.

Section 8: Auditing and Accountability

These questions describe technical safeguards and security measures:

How is the information in the project, application, or system secured?

The CEC-IOD-System Security Branch (SSB) implements a rigorous Audit Logging Program. The Audit Logging Group normalizes system event log files and forwards them [daily] to the Security Operation Center who reviews and enters each event into the Simple Oracle Document Access (SODA)-database. Logs are maintained for a minimum of 6 months. Audit records are reviewed and analyzed for inappropriate or unusual activity on a daily basis. Any findings of inappropriate activity is escalated to members of the audit logging team for further review. Audit review, analysis, and reporting are adjusted if a change in risk threshold is identified. The CEC Enterprise Active Directory (EAD) system uses the baseline high impact security controls from NIST SP 800-53 Revision 4 in establishing security mechanisms to protect the system. This includes network perimeter border protection, auditing and alerting for tracking and monitoring events on the system.

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

Individual users have individual user access accounts that do not access the EAD system. Individual user access accounts are listed in the Active Directory-Directory Services module. The EAD system is only accessible by privileged account holders holding specific account roles. Account Management Standard Operating Procedures are documented and include that Privileged account holders must complete a background investigation, and a completed agency access process must be completed prior to being given access to the system.

The EAD system utilizes the following default account roles:

- Account Operators
- Administrators
- Allowed RODC Password Replication Group
- Backup Operators
- Cert Publishers
- Certificate Service DCOM Access
- Cryptographic Operators
- Denied RODC Password Replication Group
- Distributed COM Users
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users

- Enterprise Admins
- Enterprise Read-only Domain Controllers
- Event Log Readers
- Group Policy Creator Owners
- Guests• IIS_IUSRS
- Incoming Forest Trust Builders
- Netmon Users
- Network Configuration Operators
- Performance Log Users
- Performance Monitor Users
- Pre-Windows 2000 Compatible Access
- Print Operators
- RAS and IAS Servers
- Read-only Domain Controllers
- Remote Desktop Users
- Replicator
- Schema Admins
- Server Operators
- Terminal Server License Servers
- Users
- Windows Authorization Access Group

The EAD system utilizes additional account roles as defined by the EAD Functional Specification and delegated to agency Organizational Unit (OU).

How does the project, application, or system review and approve information sharing requirements?

Information Sharing between systems is pre-determined and goes through series of review and approvals via Interconnection Security Agreements (ISAs). Information sharing with users are strictly controlled and protected by user roles and responsibilities and needs to know basis.

Describe what privacy training is provided to users either generally or specifically relevant to the project, application, or system.

The USDA OCIO mandates annual Privacy training. AgLearn provides security and awareness training to all employees/contractors initially upon hiring and on an annual basis.