# 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 | OO-Mail Modernization System (OOMMS) |
| Program Office | Office of Operations (OO) |
| Mission Area | Departmental Administration Information Technology Office (DAITO) |
| CSAM Number | 2718 |
| Date Submitted for Review | 9/30/2025 |

# Mission Area System/Program Contacts

| Role | Name | Phone Number |
|---|---|---|
| MA Privacy Officer | Nija Enclarde | - |
| Information System Security Manager | Lisa McFerson | 202-720-8599 |
| System/Program Managers | Chris Betner | 202-505--0630 |

# Abstract

USDA Headquarters receives 5,000 mail pieces from USPS every day. Mail that is ¾ inch thick or less undergoes screening through Tritek's "Threat Detect" system. The OO-Mail Modernization System (OOMMS) system promptly identifies any mail containing Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE-Defense) CBRNE-D threats, and has protocols in place for USDA personnel to isolate all compromised items.

OOMMS aims to create a safer and more efficient communication environment for USDA employees. The purpose of this system is to enhance the safety and efficiency of mail handling at the USDA by:

- Testing Incoming Mail: Screening for drugs, chemicals, and biological particles to protect employees and ensure workplace safety.
- Expediting Document Delivery: Improving the speed of delivering critical documents, which is particularly important in a hybrid workplace environment.
- Digitizing Communications: Transitioning to digital formats to streamline communication processes and improve accessibility.
- Employee Choice: Allowing USDA employees to choose how they prefer to receive business communications, thereby increasing flexibility and responsiveness.

# Overview

The OO-Mail Modernization System (OOMMS) system promptly identifies any mail containing Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE-Defense) CBRNE-D threats, and has protocols in place for USDA personnel to isolate all compromised items. The OOMMS system leverages the ICAM Shared Services (eAuth) PIA for the PII contained in its system. OOMMS aims to create a safer and more efficient communication environment for USDA employees. The purpose of this system is to enhance the safety and efficiency of mail handling at the USDA by screening for drugs, chemicals, and biological particles to protect employees and ensure workplace safety; improving the speed of delivering critical documents, which is particularly important in a hybrid workplace environment, transitioning to digital formats to streamline communication processes and improve accessibility, and allowing USDA employees to choose how they prefer to receive business communications, thereby increasing flexibility and responsiveness.

# 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?**

E-Government Act (2002): Establishes guidelines for federal information technology and electronic government services.

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

No

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

Privacy Impact Assessment ICAM Shared Services, 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? Select all applicable**

Biographical Information:

- Name (Including Nicknames)
- Business Mailing Address (Sole Proprietor)
- Home Address
- ZIP Code
- Personal Email Address
- Business Email Address

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

USDA staff/mail receipts information is collected through USDA's ICAM and Active Directory systems. Mail sender's name and address is captured via mail scanning process that reads information from the front and back of the envelope and also the mail content.

**How is the information collected?**

USDA staff/mail receipts information is collected through USDA's ICAM and Active Directory systems. Mail sender's name and address is captured via mail scanning process that reads information from the front and back of the envelope and also the mail content.

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

No.

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

USDA's ICAM and Active Directory based data is checked for accuracy at source systems. OO-MMS does not check or modify this data.

Mail sender's information is not checked by the system for accuracy as this is the responsibility of the sender.

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

No

**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

**List the privacy risks and mitigations related to the characterization of the information.**

**Privacy Risk**: Inadequate Security Controls: PII that is not properly characterized may not be prioritized for protection, making it more vulnerable to breaches and unauthorized disclosures.

**Mitigation**: Access Controls: Implement Role-based Access Controls based on the classification of information, ensuring that only authorized personnel can access sensitive data.

# 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.**

Information that is collected, used and disseminated and/or maintained with support the following business functions for USDA operations.

Testing Incoming Mail: Screening for drugs, chemicals, and biological particles to protect employees and ensure workplace safety.

Expediting Document Delivery: Improving the speed of delivering critical documents, which is particularly important in a hybrid workplace environment.

Digitizing Communications: Transitioning to digital formats to streamline communication processes and improve accessibility.

**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.**

System does collect mail related data to include senders' information, recipients' information and the mail content. System does allow these data elements to search for proper handling and dissemination of the data and to provide accurate reporting as per business needs, such as number of mails received, delivered, rejected, or caught in Threat Detection phases. The data collected can be used to predictive patterns or anomaly such as Threat Detection found in incoming several mails and from various addresses.

**List the privacy risks and mitigations related to uses of the information.**

**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.

**Mitigation**: Regular Training: Provide regular IT security awareness training as part of the USDA IT policies for employees on privacy laws and the importance of adhering to the defined uses of personal information to ensure compliance.

# 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?**

When mail is sent to USDA, the information collected is voluntarily provided to USDA by the sender as with any paper-based mail processing and delivery processes.

Mail recipients in USDA do provide consent to use their names and business addresses as part of the HR processes and governmental business requirements.

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

N/A.

**List the privacy risks and mitigations 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**: Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

# 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?**

NARA's email retention policy, the "Capstone" approach, mandates permanent retention of email records for designated officials due to their high-level decision-making roles, transferring them to the National Archives. For all other federal employees, a 7-year retention is standard. However, this information is also retained in USDA's Exchange/email servers as all the communication and data is passed to recipients via it.

**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.**

Yes. The approved records schedule for these items is: Department of Agriculture, Office of the Secretary of Agriculture [Capstone Form]. The schedule includes two disposition authorities:

- GRS-6-1-0016-2023-0001, Item 10 for permanent records; and
- GRS-6-1-0016-2023-0001, Item 011 for temporary records.

**List the privacy risks and mitigations related to data retention.**

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

**Mitigation**: 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.

# 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?**

System is interfaced with USDA's Exchange server for email processing, and ICAM system for user access authentication.

**List the privacy risks and mitigations related to internal information sharing and disclosure.**

**Privacy Risk**: Unauthorized Access: Employees may access PII without proper clearance, leading to potential misuse.

**Mitigation**: Access Controls: Implement role-based access controls to limit who can access PII based on their job responsibilities.

**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?**

None.

**List the privacy risks and mitigations related to external information sharing and disclosure.**

**Privacy Risk**: N/A

**Mitigation**: N/A

# 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?**

Only USDA employees and contractors will have authorized access to their data and related information after getting authenticated and authorized by ICAM-eAUTH access mechanisms.

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

System does not allow for modifications to the data that is fed in the system on PII level as data is collected from other USDA systems and paper-based envelopes received for mail routing.

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

If a user finds inaccurate PII information of their own, they will need to work with HR and ICAM-eAUTH systems to get the data corrected. OO-MMS does not allow PII data corrections.

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

N/A within the system.

**List the privacy risks and mitigations 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.

**Mitigation**: Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

# Section 8: Auditing and Accountability

These questions describe technical safeguards and security measures:

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

Data is secured and hosted in CEC's AZURE cloud hosting service provider. Only authorized users can access the system/data while remaining in the USDA network/eVPN and after authenticated by ICAM-eAUTH system.

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

Business Owner will be working with the technical teams to prepare and manage System's User Account Management document that will outline the roles, groups, user level access privileges and the account recertification process for privileged users.

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

System Narrative, Business Impact Analysis and Design documents are regularly reviewed and updated as per Information Security/ATO policies and guidelines.

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

All users who have access to the system must go through IT security awareness training as part of the USDA IT policies.