USDA Privacy Impact Assessment

Fiscal Year 2024

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.”
05/21/2025	1.2	OSSOLVE PIA Updates by ISSO

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	Onsolve Platform System. (OP1)
Program Office	IRMC
Mission Area	DAITO
CSAM Number	2701
Date Submitted for Review	

Mission Area System/Program Contacts

Role	Name	Email	Phone Number
MA Privacy Officer	Please Provide	Nija.enclarde@usda.gov	318-955-1393
Information System Security Manager	Lisa McFerson	Lisa.McFerson@USDA.gov	202-720-8599
System/Program Managers	James Hughes	*James.hughes@usda.gov*	202-692-0266

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 Onsolve Platform (OP) is an emergency notification system used by agencies to send notifications to employees about emergency situations and Continuity of Operations Plan.

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 Onsolve Platform (OP) system sends out notifications to USDA employees for agency defined emergencies or issues. Multiple agencies use the system they include:

- Agricultural Marketing Service (AMS)
- Farm Production and Conservation Business Center
- Farm Service Agency (FSA)
- Food Safety Inspection Service (FSIS)
- Food, Nutrition, and Consumer Services (FNCS)
- Natural Resources Conservation Services (NRCS)
- Office of Chief Financial Officer (OCFO)
- Office of General Counsel (OGC)
- Office of the Chief Information Officer (OCIO)
- Office of the Inspector General (OIG)
- Risk Management Agency (RMA)
- Rural Development (RD)
- Office of Homeland Security

Section 1: 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?

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; eGovernment Act of 2002 (H.R. 2458/Pub. L. 107– 347); GRAMM-LEACH-BLILEY ACT (Pub L. 106–102)

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

Yes, expires 12/5/2026

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

USDA/OCIO-2 eAuthentication Service

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

Yes

Section 2: 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 in 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
☐ Passport number	☐ License Plate number	☐ Registration number
☐ File/Case ID number	☐ Student ID number	☐ Federal Student Aid number
☐ Employee Identification number	☐ Alien Registration number	☐ DOD ID 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

☐ Health Plan Beneficiary number
☐ Business Mobile number (sole proprietor)
☐ DOD Benefits number

Biographical Information

☒ Name (Including Nicknames)
☐ 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
☐ Religion/Religious Preference

☐ Citizenship
☐ Immigration Status
☒ Home Phone or Fax Number

☐ Home Address
☒ ZIP Code
☐ Marital Status

☐ Spouse Information
☐ Children Information
☐ Military Service Information

☐ Race
☐ Nationality
☐ Mother's Maiden Name

☒ Personal Email Address
☒ Business Email Address
☒ Global Positioning System (GPS)/Location Data

☐ Employment Information
☒ Alias (Username/Screenname)
☐ Personal Financial Information (Including loan information)

☐ Education Information
☐ Resume or Curriculum Vitae
☐ Business Financial Information (Including loan information)

☐ Professional/Personal References

Biometrics

☐ Fingerprints
☐ Hair Color
☐ DNA Sample or Profile

☐ Retina/Iris Scans
☐ Video Recording

Distinguishing Features

☐ Palm Prints	☐ Eye Color	☐ Signatures
☐ Dental Profile	☐ Photos	

Characteristics

☐ Vascular Scans	☐ Height	☐ Weight
☐ Scars, Marks, Tattoos	☐ Voice/Audio Recording	

Device Information

☐ Device Settings or Preferences (e.g., Security Level, Sharing Options, Ringtones)	☐ Cell Tower Records (e.g., Logs, User Location, Time)	☐ Network Communication Data

Medical /Emergency Information

☐ Medical/Health Information	☐ Mental Health Information	☐ Disability Information
☐ Workers' Compensation Information	☐ Patient ID Number	☐ Emergency Contact Information

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

[List additional information collected but not listed above here (for example, a personal phone number that is used as a business number).]

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

Enterprise Identity Management System (EIMS) and the Remedy database, Onsolve Platform System.

2.2.1. How is the information collected?

When employees are hired HR records and System Authorization Access Request (SAAR) are entered. The Remedy system is updated, and both sets of data are sent in CSV files. A script is run to put the data together. Agency leads may collect personal mobile phones and email addresses

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

No

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

EIMS is the HR system and Remedy is tied to the Enterprise Active Directory. Users can self-service to provide updates. The file will be uploaded to OP once a week

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

No

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

N/A

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

None

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

Follow the format below:

Privacy Risk: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Mitigation: Implement access controls based on the classification of information, ensuring that only authorized personnel can access sensitive data.

Section 3: 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 uploaded into OP using a CSV file with EIMS and Remedy data. It is then loaded weekly into the system. The data is used to contact USDA employees in an emergency or COOP activities.

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.

No

3.3. **Privacy Impact Analysis**: Related to uses of the information.

Follow the format below:

Privacy Risk: Using PII beyond its intended purpose can increase the risk of data exposure and violate privacy regulations.

Mitigation: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

Section 4: Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses 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?

There is a privacy statement provided for self-service for employees and the listed SORN USDA/OCIO-2 eAuthentication Service.

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

Individuals have the right to decline to provide personal information such as home phone, cellular and home email address.

4.3. **Privacy Impact Analysis**: Related to notice.

Follow the format below:

Privacy Risk: If notices do not clearly explain the purpose of data collection, individuals may be more likely to provide information that is not necessary, leading to potential data minimization violations.

Mitigation: Limit data collection to only what is necessary for the stated purpose. Avoid collecting excessive or irrelevant data.

Section 5: 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?

Contact information is being retained along with a history of emergency alerts that have been sent out using the system.

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.

No

5.3. **Privacy Impact Analysis**: Related to retention of information.

Follow the format below:

Privacy Risk: Retained data may become outdated or irrelevant, leading to inaccuracies in decision-making or service delivery, which can affect individuals negatively.

Mitigation: Collect and retain only the PII that is necessary for the intended purpose, minimizing the risk associated with holding excessive data.

Section 6: 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?

No information is being shared with other agencies or offices. Every agency or office has access to their contacts and only their contacts. The application has the ability to allow everyone to see all, but OCIO has controls in place to prevent that.

6.2. **Privacy Impact Analysis**: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: Internal systems can be vulnerable to breaches, compromising PII.

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

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?

Information is not being shared outside of USDA.

6.4. **Privacy Impact Analysis**: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk: Information is not being shared outside of USDA

Mitigation: Information is not being shared outside of USDA

Section 7: 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?

Users can use a self-service portal to verify their contact information. They can provide some personal information like a mobile phone number or a home email. Any other changes they must contact HR and put in a SAAR request.

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

Data comes from HR and Remedy so self-service URL is provided.

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

Administrators will notify their agencies.

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

N/A

7.5. **Privacy Impact Analysis**: Related to redress.

Follow the format below:

Privacy Act risks associated with redress include:

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: By implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

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

User Awareness Campaigns: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.

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?

The system is a FedRamp solution and will have related security documents. Users must use their LincPass to access the system.

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

Agencies provide emergency coordinators through their leadership. System owners assign roles to those users to manage their agencies.

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

Agency coordinators approve information

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

Annual Information Security Awareness, and Privacy training is provided by USDA.

Privacy Impact Assessment Review

[USDA Privacy Office completes this section.]

Date reviewed by USDA Privacy Office: 6/17/2025

USDA Privacy Analyst (On behalf of USDA's Chief Privacy Officer):

Signed: TRACY HENDRIX Digitally signed by TRACY HENDRIX Date: 2025.06.25 22:40:30 -04'00'

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Signed:_____

James Hughes
System Owner
Office of the Chief Information Officer
U.S. Department of Agriculture

Signed:_____

Nija Enclarde
Mission Area Privacy Officer
Departmental Administration Information Technology Office
U.S. Department of Agriculture

Signed:_____

Sullie Coleman
ACISO
Departmental Administration Information Technology Office
U.S. Department of Agriculture