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.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project 3
Mission Area System/Program Contacts 3
Abstract 4
Overview 4
Section 1: Authorities and Other Requirements 7
Section 2: Characterization of the Information 8
Section 3: Uses of the Information 10
Section 4: Notice 11
Section 5: Data Retention 12
Section 6: Information Sharing 14
Section 7: Redress 15
Section 8: Auditing and Accountability 16

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	DM-AG-Automated Warning and Information Response System (DM AG-AWalRS)
Program Office	Office of Safety, Security and Protection (OSSP)
Mission Area	Department Administration Information Technology Office (DAITO)
CSAM Number	1977
Date Submitted for Review	August 26, 2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Nija Enclarde	(318) 955-1393
Information System Security Manager	Lisa McFerson	(202) 720-8559
System/Program Managers	Bryan Mulvenna	(202) 378-2568

Abstract

The DM-AG-Automated Warning and Information Response System (AG-AWaIRS) application is used to enhance existing procedures for emergency planning and notification. The Ag-AWaIRS application utilizes the internet/intranet to notify personnel of emergencies, building-related alerts and messages via text messages, email, and desktop popup alerts.

Overview

The Agriculture Automated Warning and Information Response System (Ag-AWaIRS), is a Government-owned, fully licensed, commercial-off-the-shelf (COTS) application, IWSAlerts™ acquired from AtHoc, a division of BlackBerry, that is an enterprise class emergency notification system, allowing a distributed organization to alert different groups using different alerting devices, including desktop popups, voice telephony, text messages, email, and other devices. Ag-AWaIRS is not publicly accessible.

Ag-AWaIRS tracks alert distribution and responses and provides its operators with online reports showing the progress of alert dissemination. Ag-AWaIRS operators connect via a secure and permission-based web user interface to perform alert creation, initiation, and administration tasks. AG-AWaIRS end-users can use its secure web-based self-service to view past and current alerts, and view and update their work-related contact information. A high-level depiction of the information flow in the system is shown below.

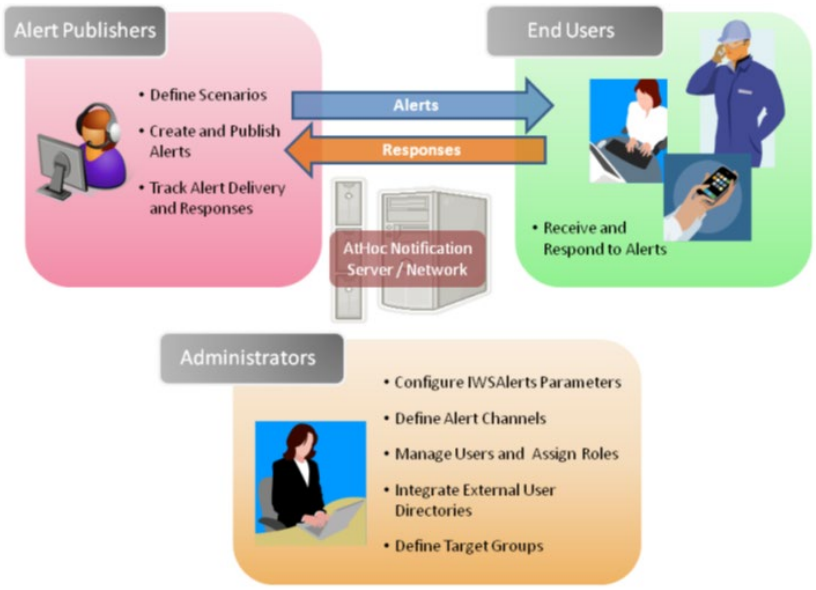

Figure 1: Ag-AWaIRS Process Flow

IWSAlerts™ can integrate with organizational personnel databases to collect and update user data, including user attributes and contact details. IWSAlerts™ can connect with multiple alerting sources, including Weather Alerts coming from the National Oceanic and Atmospheric Administration (NOAA) and National Weather Service (NWS) and local fire panels, video surveillance, and more. The system

architecture supports high availability via a failover configuration, with local and distributed redundancy.

The IWSAlerts™ software is designed to establish and distribute alerts on the Local Area Network (LAN) to all desktop clients, and to additional devices such as phone, mobile devices, and email. AG- AWaIRS provides USDA organizations with the ability to rapidly and effectively disseminate threat response information throughout the network environment, including signals, watches, warnings, evacuation routes and other alerting information to meet NIST and federal warning requirements.

Ag-AWaIRS is a server-based system, which allows a client application (installed on end-user's desktops) to periodically connect, using HTTPS, to the Ag-AWaIRS server and fetch pending alerts, if any. Once an alert is available, it is rendered on the end-user desktop as a Desktop Popup Alert (a.k.a. Desktop Notifier) and transmitted via other delivery devices such as phone, email, and mobile devices. Responses are continuously gathered and tracked, to provide an alert delivery report. A web-based management system (administration console) enables authorized users to publish alerts to end-users and view reports. Refer to Figure 2: IWSAlerts™ High Level Interconnection Architecture for further information on the system architecture.

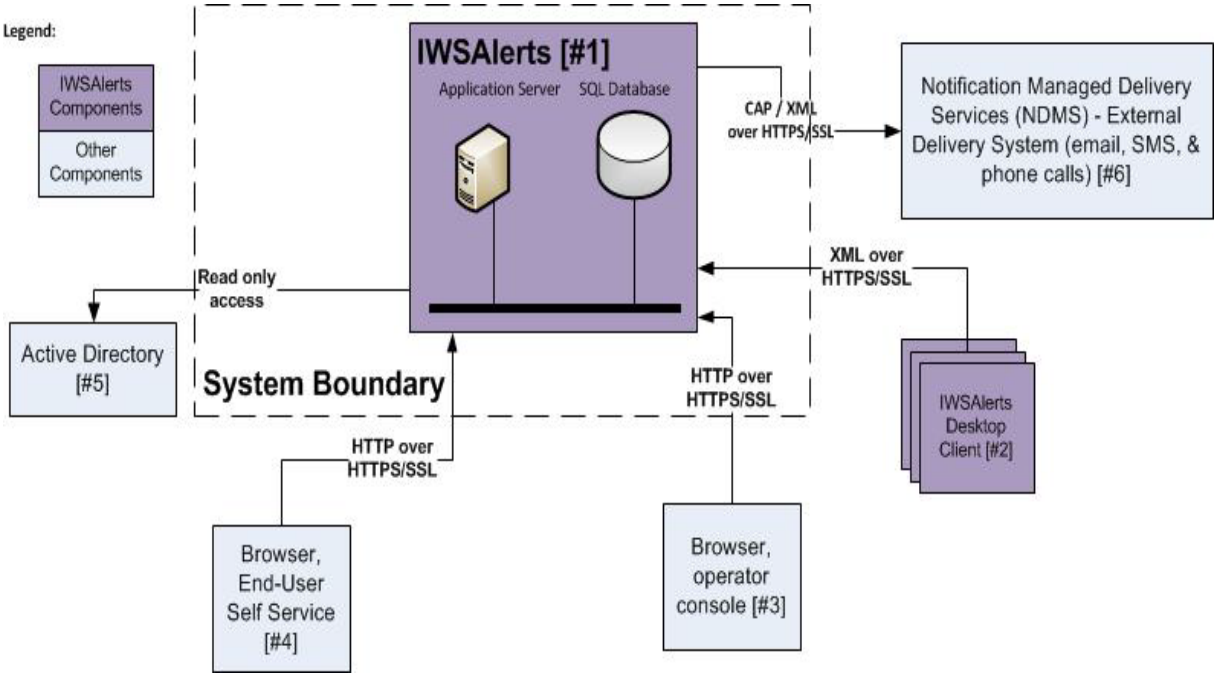

Figure 2: IWSAlerts™ High Level Interconnection Architecture

Ag-AWaIRS transforms the USDA IP network into an enterprise-class mass notification system. Through the deployment of Ag-AWaIRS, the Office of Operations can rapidly alert thousands of employees in geographically dispersed buildings and facilities during an emergency.

Ag-AWaIRS provides:

- Personnel protection: Mass dissemination of alerts across multiple channels, accelerating threat response
- Personnel recall: Rapid communication with off-facility personnel to report back to duty

- Personnel accountability: Real-time response tracking reports on the status and safety of all personnel
- Critical communications: Distribute important Department information to employees, including IT mass alerting
- Regulatory compliance: Meets government and commercial emergency management, disaster recovery, and continuity planning requirements, including fire and building safety (e.g., NFPA 72 2010)

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.

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

5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347 (Ethics in Government Act of 1978), and Executive Orders 9397, as amended by 13478, 9830, and 12107

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

Yes. This system currently has an ATO with Conditions dated 3/28/2025 and currently going through a complete ATO.

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

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

No

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.

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

Identifying Numbers:

- Personal Mobile number

Biographical Information:

- Name (Including Nicknames)
- Group Organization/Membership
- Zip Code
- Business Email Address

Specific Information/File Types:

By default, the system only collects the network username of the recipient (i.e., usda\johnsmith). However, optionally, end-users can update their accounts to include government issued cell/text numbers, government email address, personal cell/text numbers, and personal email addresses.

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

USDA Active Directory

How is the information collected?

Initially during computer login to USDA network. Additional details collected via self-update.

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

No

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

It is the end-user's (message recipient) responsibility to maintain.

Does the system/program 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?

None

Privacy Impact Analysis: Related to characterization of the information.

Privacy Risk: Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

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.

Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

Information collected and maintained by the end-user will help ensure life-safety during a man-made or natural disaster. It will be used to disseminate emergency messaging, as appropriate, via desktop popup alerts, text, and email messaging.

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

Privacy Impact Analysis: Related to uses of the information.

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

Mitigation: Transparency: Inform individuals about how their personal information will be used, including any potential secondary uses, through clear and accessible privacy notices.

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.

How does the project/program/system provide notice to individuals prior to collection?

N/A

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

End-users are not required to provide any information. Self-update is 100% optional.

Privacy Impact Analysis: Related to notice.

Privacy Risk: Failure to Communicate Changes: Not adequately informing individuals about changes to privacy practices or policies can lead to confusion and mistrust, especially if data practices evolve.

Mitigation: Feedback Mechanism: Establish a process for users to ask questions or express concerns about privacy notices and practices, allowing for continuous improvement.

Section 5: Data Retention

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

What information is retained and for how long?

Information is retained for 90 days after separation of duty to USDA. Accounts can also be removed per user or HR request to the system admin.

- General Records Schedule 3.2: Information Systems Security Records
  - Item 030, System access records.
  - Temporary.
  - Disposition Authority: DAA-GRS-2013-0006-0003
  - Destroy when business use ceases.
  - Records Description:
  - These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
- General Records Schedule 5.2, Transitory and Intermediary Records
  - Item 020, Intermediary Records.
  - Temporary.
  - Disposition Authority: DAA-GRS-2022-0009-0002
  - Disposition Instructions: Destroy upon creation or update of the
  - final record, or when no longer needed for business use, whichever is later.
  - Records Description:
  - Intermediary records. Records that meet the following conditions:
    - They exist for the sole purpose of creating a subsequent record and
    - They are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making.
- General Records Schedule 5.3, Continuity and Emergency Planning Records
  - Item 020, Employee emergency contact information.
  - Temporary.
  - Disposition Authority: DAA-GRS-2016-0004-0002
  - Destroy when superseded or obsolete, or upon separation or transfer of employee.
  - Records Description: Records used to account for and maintain communication with personnel during emergencies, office dismissal, and closure situations. Records include name and emergency contact information such as phone numbers or addresses. Records may also include other information on employees such as responsibilities assigned to the individual during an emergency situation.

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.

Yes, the Departmental Records Officer has reviewed and provided the related records retention schedules:

- General Records Schedule 3.2, Information Systems Security Records
  - Item 030, System access records.
- General Records Schedule 5.2, Transitory and Intermediary Records
  - Item 020, Intermediary Records.
- General Records Schedule 5.3, Continuity and Emergency Planning Records
  - Item 020, Employee emergency contact information.

Privacy Impact Analysis: Related to retention of information.

Privacy Risk: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

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

The following questions are intended to define the content, scope, and authority for information sharing.

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?

Information is received via Active Directory but only includes network name (i.e., usda\joesmith) Information is not shared by this system. Admins have access to information via SSL. Users are only given rights to update their profile and pull alerts from the agents (no database or web application access).

Privacy Impact Analysis: Related to internal sharing and disclosure.

Privacy Risk: Information is not shared by this system.

Mitigation: Information is not shared by this system.

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 shared externally by this system.

Privacy Impact Analysis: Related to external sharing and disclosure.

Privacy Risk: Information is not shared, received or transmitted externally.

Mitigation: Information is not shared, received or transmitted externally.

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.

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

Information is provided and/or updated by the end-user through the agency application installed on the taskbar of USDA issued devices.

What are the procedures for correcting inaccurate or erroneous information?

Information is provided and/or updated by the end-user through the agency application installed on the taskbar of USDA issued devices.

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

A self-update guide is available, but users are responsible for maintaining their own information.

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

Individuals can email Ag-AWaIRS-Support@usda.gov for assistance updating contact information.

Privacy Impact Analysis: Related to redress.

Privacy Risk: Failing to provide adequate redress options may expose mission areas or agencies to legal challenges, including lawsuits or regulatory scrutiny, especially if individuals feel their rights have been violated.

Mitigation: Implement protocols for acknowledging and responding to redress requests promptly, ensuring that individuals feel heard and valued

Section 8: Auditing and Accountability

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

How is the information in the system/project/program secured?

The system requires level 4 multifactor authentication into the USDA network. Additionally, data is secured via encryption at rest and in transit.

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

Program access is based on agency needs and approved by senior leadership. They are documented via email.

How does the program review and approve information sharing requirements?

The system gets a nightly feed from Identity Credential and Access Management (ICAM) program that provides employee information which is used to identify the division and building assignment for individuals as well as provide the ability to use Single Sign On (SSO).

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

USDA Information Security Awareness Training & Acknowledgment of Rules of Behavior are required by all federal employees and contractors. Privacy and PII training is included in the Security Awareness and Rules of Behavior training required for all federal employees and contractors annually. An exam is provided following the training, and the user must receive 70% or better to maintain or receive access to the information system.