

Privacy Impact Assessment

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: November 23, 2020
- Prepared for: USDA OCIO-Police, E-Government and Fair Information Practices (PE&F) in support of DAAG-Automated Warning and Information Response System (DA Ag-AWaIRS)





Privacy Impact Assessment for the

**DM-AG-Automated Warning and Information Response System
(DM AG-AWaIRS)**

11/23/2020

Contact Point

Bryan Mulvenna

**Emergency Management Specialist
Office of Safety, Security and Protection
Safety, Training and Emergency Management
United States Department of Agriculture
202-368-1378**

Bryan.Mulvenna@usda.gov

Reviewing Official

Tariq Khalil

**Information System Security Manager
Office of the Chief Information Officer
Departmental Administration Information Technology Office
United States Department of Agriculture
202-205-2896**

Tariq.Khalil@usda.gov



Abstract

The DM-AG-Automated Warning and Information Response System (DM AG-AWaIRS) application is used to enhance existing procedures for emergency planning and notification. The Ag-AWaIRS application notifies USDA personnel of emergencies, building-related alerts and messages in a designated environment.

This PIA is being conducted because the system collects USDA personnel name, work phone numbers email.

Overview

AG-AWaIRS is owned by the Office of Safety, Security and Protection (OSSP). The designated system owner is Jeffrey Sheckels.

General System Description/Purpose

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 (www.athoc.com), 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, and text messages to mobile devices, email, telephone systems, 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 in Figure 1.6.1: AG-AWaIRS' Process Flow.

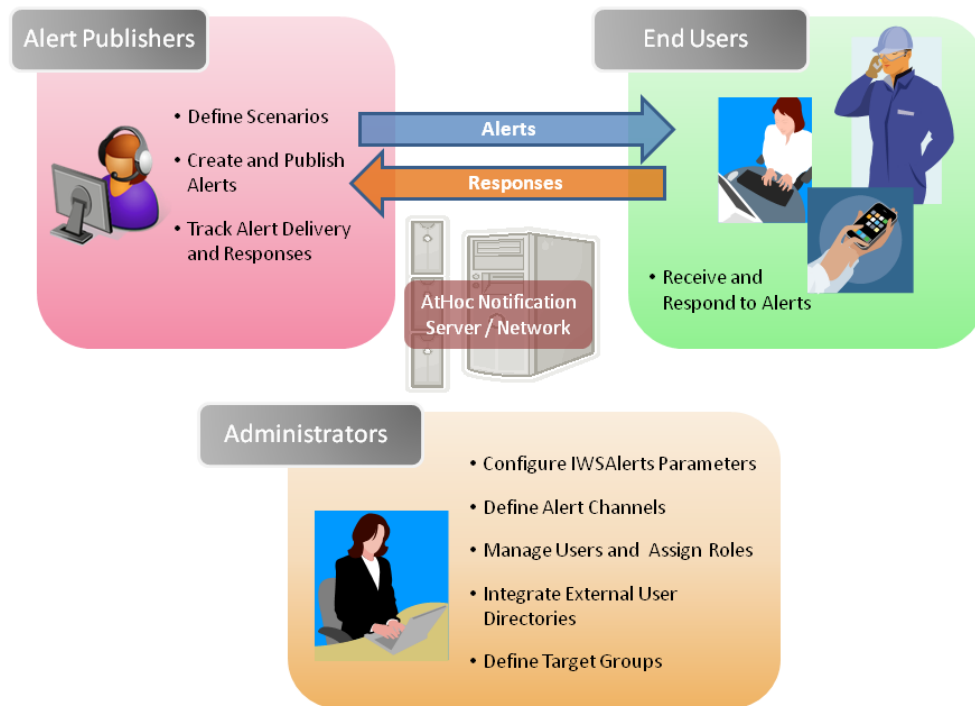


Figure 2.6.1: AG-AWaIRS' Process Flow

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 1.6.2: IWSAlerts™ High Level Interconnection Architecture for further information on the system architecture.

Each of the components shown below is described in Section 1.7.3, System Architecture Description.

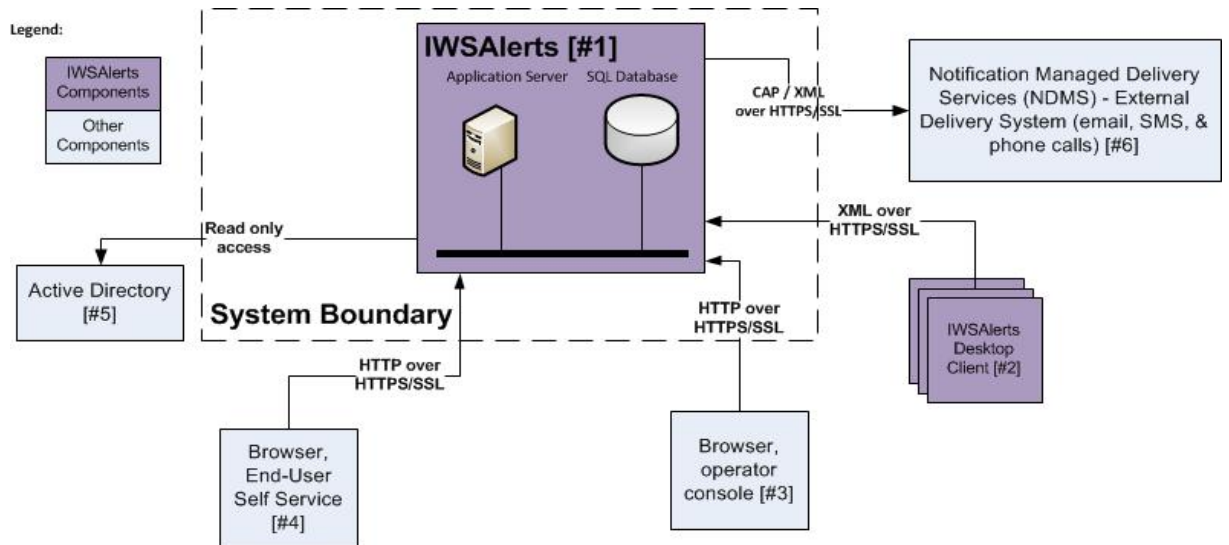


Figure 2.6.2: IWSAlerts™ High Level Interconnection Architecture

AG-AWaIRS transforms the USDA IP network into an enterprise-class mass notification system. Through the deployment of AG-AWaIRS, 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 to 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)

For System Assessment and Authorization (A&A) purposes the system is classified as a Minor Application in CSAM with a MODERATE designation for concerns for Confidentiality, Integrity and Availability. The production system is located at the Digital Infrastructure Services Center (DISC), 8930 Ward Parkway, Kansas City, MO, 64114.

The system does not conduct any information sharing.

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?

USDA personnel name, address information and work phone numbers.

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

Personnel enter their information themselves.

1.3 Why is the information being collected, used, disseminated, or maintained?

To provide USDA personnel with emergency alerts and notifications.

1.4 How is the information collected?

Personnel voluntarily enter their information into the system.

1.5 How will the information be checked for accuracy?

The system does not check user input for accuracy.

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

Jeffrey Sheckels, Director of Safety, Training and Emergency Management within the office of safety, Security and Protection approved the collection of information for this system.

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

There is a risk of a loss of confidentiality to personnel name, address information and phone. This is mitigated through the encryption of data at rest and in transit. In addition, access to the system requires a level 4 multifactor authentication into the USDA network.

Important to note: This information is publicly available on the USDA directory web page: <https://offices.sc.egov.usda.gov/employeeDirectory/app>

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.

Emergency Notifications to personnel

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

Data is not analyzed.

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

Commercial or publicly available data are NOT used.

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

Data encryption for data in transit and at rest. In addition, access to the system requires a level 4 multifactor authentication into the USDA network.

Section 3.0 Retention

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

3.1 How long is information retained?

Account profiles are deleted after 90 days of inactivity.

Account profiles can also be removed per user/HR request to the system admin.

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

N/A

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

Minimal risk identified since the data is encrypted. Access to the data is only granted to system admins

Section 4.0 Internal Sharing and Disclosure

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

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

Information is not shared by this system

4.2 How is the information transmitted or disclosed?

Information is not shared by this system. Admins have access to the information via SSL. Users are only given rights to update their profile and pull alerts from the agents (no database or web application access).

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

N/A

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, what information is shared, and for what purpose?

Information is not shared externally by this system

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 the program or system can share the personally identifiable information outside of USDA.

N/A

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

N/A

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

N/A

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 Was notice provided to the individual prior to collection of information?

No

6.2 Do individuals have the opportunity and/or right to decline to provide information?

Yes. Users may update or remove their information at any time using the agent software on their government issued desktop. In addition, users receive notification every 90 days to update their information.

6.3 Do individuals have the right to consent to uses of the information? If so, how does the individual exercise the right?

Yes, users may add, remove or update their information through the agent application installed on the task bar of the USDA issued devices.

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

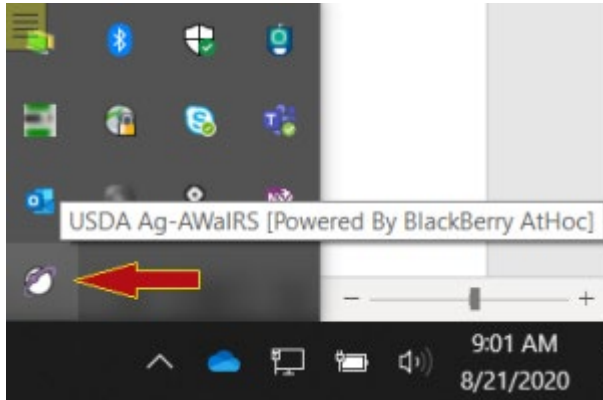
Quarterly notice for users to update their information is distributed via desktop pop up and email

Section 7.0 Access, Redress and Correction

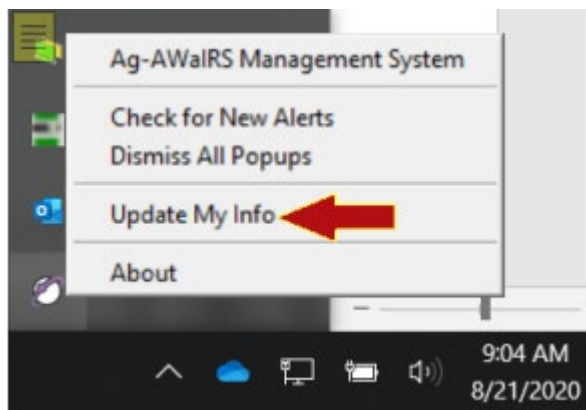
The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

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

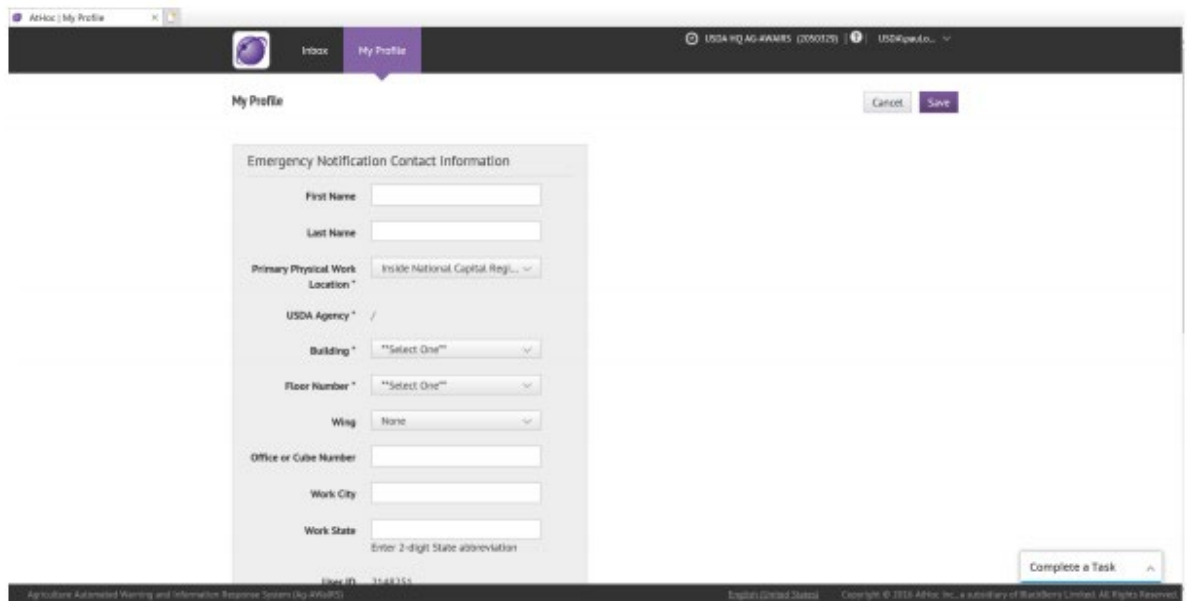
1- After authenticated to the USDA network using multi-factor authentication, users can access the AG-AWaIRS client from the task Bar. Right click on the AG-AWaIRS icon



2- *Select update my info*



3- Users update thir profile and save



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

Users will need to follow the instruction illustrated above to correct their information.

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

Quarterly notification was sent to users to update their information.

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

N/A

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

All users are required to authenticate into the USDA network via Level 4 Multifactor authentication before being provided authorization to edit their data on AG-AWaiRS.

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 access the system and are they documented?

Client application (installed on end-user desktops) periodically connect, using HTTPS, to the AG-AWaIRS server and pull pending alerts, if any.

8.2 Will Department contractors have access to the system?

Contractors authorized to have a domain network account will have access to the application agent. Access to the system management plane and database is restricted to the system admin only.

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

The agent is available to all USDA personnel. Each agency will administer privacy training at their own discretion. OSSP does not administer privacy training to users

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

Yes

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

The system employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

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

Privacy risk identified is the unauthorized disclosure of user data. This is mitigated through defense in depth provided by DISC Midrange System (Platform as a Service Hosting solution). In addition, the data is encrypted while at rest and in transit.

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?

AG-AWaIRS is a major application system.

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

NO

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 of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?**

The application does not use third party websites.

- 10.2 What is the specific purpose of the agency’s use of 3rd party websites and/or applications?**

N/A

- 10.3 What personally identifiable information (PII) will become available through the agency’s use of 3rd party websites and/or applications.**

N/A

- 10.4 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?**

N/A

- 10.5 How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be maintained and secured?**

N/A

- 10.6 Is the PII that becomes available through the agency’s use of 3rd party websites and/or applications purged periodically?**

N/A

- 10.7 Who will have access to PII that becomes available through the agency’s use of 3rd party websites and/or applications?**

N/A

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

N/A



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

N/A

10.10 Does the system use web measurement and customization technology?

N/A

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

N/A

10.12 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.

N/A

Agency Responsible Officials

Jeffrey Sheckels
DA/OSSP
United States Department of Agriculture

Agency Approval Signature

Lisa McFerson
Information Systems Security Manager
Departmental Administration Information Technology Office
United States Department of Agriculture