

OpenNet Windows Active Directory (WINAD) PIA

1. Contact Information

A/GIS Deputy Assistant Secretary

Bureau of Administration

Global Information Services

2. System Information

- (a) Name of system: OpenNet Windows Active Directory
- (b) Bureau: Information Resource Management (IRM/OPS/ENM/NED)
- (c) System acronym: WINAD
- (d) iMatrix Asset ID Number: 633
- (e) Reason for performing PIA: Click here to enter text.
 - New system
 - Significant modification to an existing system
 - To update existing PIA for a triennial security reauthorization

Explanation of modification (if applicable): 1. Introduction of Windows 2012 R2 and Windows 2016 Domain Controllers. Windows 2008 R2 domain controllers are gradually being replaced. 2. Extension of the Active Directory Domain Services authentication system to cloud applications using Active Directory Federation Services. 3. Synchronization of Active Directory Domain Services user account and group information to the enterprise Department of State Azure Active Directory in the Microsoft Government Community Cloud Office 365 and to enterprise Department of State Azure Active Directory in the Microsoft Azure Government (MAG) Cloud to support DOS Azure services.

3. General Information

- (a) Does the system have a completed and submitted Security Categorization Form (SCF)?
 - Yes
 - No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

- (b) What is the security Assessment and Authorization (A&A) status of the system?

The ATO expired March 31st, 2017. WINAD remained operational despite the expired ATO as it is an essential component of the Departments network.

The assessment took longer than usual due to 1) lack of dedicated resources which resulted in overtasking; 2) resources not having the knowledge to complete task; 3)

incomplete documentation; 4) Pen Test completion and remediation; 5) delays in PIA completion.

The system is expected to receive reauthorization in May 2020.

(c) Describe the purpose of the system:

The purpose of this system is to provide identification, authentication and authorization to access the IT systems in the OpenNet environment and to authorized cloud hosted Department of State or Other Government Agency (OGA) applications.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

ITMart, Diplomatic Security's badging office, A/EX MyProfile, and other Active Directory (AD) Administrators collect and store the following PII in WINAD: federal government employee and contractor names, OpenNet e-mail address, office location, business phone number, and organizational office symbol and associated organization/company.

US Agency for International Development (USAID) AD and Bureau of Global Public Affairs (GPA) - Public Affairs Communicating Electronically (PACE) AD share their business contact information with WINAD allowing OpenNet users to easily email users in these related organizations.

The Microsoft Exchange Skype-for-Business systems can and do selectively store user photos in the WINAD database if users choose to add this information.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

44 U.S.C. 3554, (Federal Information Security Modernization Act of 2014)

44 U.S.C. 3544 (Federal Agency Responsibilities, Coordination of Federal Information Policy, Information Security)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

- SORN Name and Number:
- Network User Account Records, State-56.
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): December 12, 2017

No, explain how the information is retrieved without a personal identifier.

[Click here to enter text.](#)

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? Yes No

If yes, please notify the Privacy Division at Privacy@state.gov.

- (h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? Yes No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:

- Schedule number (e.g., (XX-587-XX-XXX)): A-03-003-04
- Length of time the information is retained in the system: 3 years
- Type of information retained in the system: Configuration Management, inventories of IT assets, problem reports and related decision documents relating to the system architecture and software infrastructure of the network or system; reports on operations including measures of benchmarks, performance indicators, critical success factors, error and exception reporting, self-assessments, performance monitoring and System Security Plan, Contingency Planning, Continuous Monitoring Strategies, and System Authorization Reports.

4. Characterization of the Information

- (a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (e.g. eligible family members, locally employed staff)

- (b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes No

- If yes, under what authorization?

[Click here to enter text.](#)

- (c) How is the information collected?

The information is collected using an Access Request form (DS-7667) either by the user or by the Government Manager. The Access Request form is used to create an OpenNet WINAD user account, which grants access to the network. The user or their Government Manager accesses IT Services online to establish a WINAD account for the user to log in and use a Department workstation, the Department's IT network and to access all appropriate IT resources at the Department. A government supervisor or authorized official must approve the request.

US Agency for International Development (USAID) Active Directory and Bureau of Global Public Affairs (GPA) - Public Affairs Communicating Electronically (PACE)

Active Directory collect and share their business contact information with WINAD allowing OpenNet users to easily email users in these other related organizations.

A/EX Myprofile performs an hourly synchronization with WINAD which provides a self service capability for users to update most of their business contact information.

Similarly, Outlook and Skype allow users to add or remove their photo from WINAD.

(d) Where is the information housed?

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

- If you did not select "Department-owned equipment," please specify.

Two instances of Azure AD are owned for the Department of State Enterprise. One is in the Microsoft Government Community Cloud (FEDRAMP moderate). The second is in the Microsoft Azure Government Cloud (FEDRAMP high).

(e) What process is used to determine if the information is accurate?

Information housed within WINAD is collected directly from each individual when they fill out an Access Request form (DS-7667) and provide it to the IT Service Center (ITSC), Consolidated Customer Support (CCS) Office, or other personnel abroad who have been delegated with the creation of WINAD accounts. This information is then populated in the Global Address List (GAL), and can be verified and corrected by the user at any given time by using the myProfile system. The continued accuracy of the information is the responsibility of the user using A Bureau's myProfile system (iMatrix# 7523) after it has been verified initially, or if reported for change by the user's Supervisor or other managerial entity to the groups listed above (ITSC, CCS, or delegated personnel).

The information populated by USAID's AD is updated hourly. The accuracy of the information is determined by USAID through their AD system internal processes to USAID.

PACE data is collected by user entry into Bureau of Global Public Affairs, PACE system, iMatrix# 895, which then performs an hourly synchronization to WINAD's AD. The accuracy of the information in PACE is determined by GPA's PACE system internal processes.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Individuals (and USAID and GPA respectively) are responsible for keeping their information up to date. If changes need to be made, Department of State employees can

request their GAL information be updated through myProfile. Users can also update their WINAD information by sending an incident request to the IT Service Ctr.

The information provided by USAID's AD and GPA Bureau's PACE AD is the responsibility of those respective Bureau's/Agencies. Synchronizations of the myProfile, USAID, and PACE data occur hourly by WINAD.

- (g) Does the system use information from commercial sources? Is the information publicly available?

No, the system does not use information from commercial resources nor is it publicly available.

- (h) Is notice provided to the individual prior to the collection of his or her information?

Yes No

DS, IT Service Center, and the POST ISSOs/OU Administrators are responsible for providing notification to the user at the point of collection, not WINAD. IT Service Center's online portal and DS-7667 (New/Transfer Account Form) are utilized for this point of collection notification process.

- (i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? Yes No

- If yes, how do individuals grant consent?

Per DS-7667 (New/Transfer Account Form): Providing the information is voluntary, but failure to provide the information may result in the delay of system logon authorization or it may be impossible for the systems staff to enter the logon credentials or user data.

- If no, why are individuals not allowed to provide consent?

- (j) How did privacy concerns influence the determination of what information would be collected by the system?

Standard business information must be utilized in order to associate a user to an account, especially when utilizing the Address Book feature of Microsoft Outlook (i.e., locating "John U. Doe" and knowing you have the right contact is possible when utilizing a first and last name, versus attempting to utilize the native AD alias of "DoeJU" which does not let you know the individual's first name and that you have found the right contact). This functionality and integration with today's business practices is inherent to the purposes of the Active Directory structure of Identification and Authentication (I&A) services. However, in general, only the minimum amount of standard business

information about an individual is collected allowing for unique identification of that individual in WINAD.

It is up to the business owners of the various systems that collect and deposit content into the WINAD system to take privacy concerns into account for managing the data that they collect and deposit, and conveying concerns/guidance to WINAD if/when appropriate for changing the current business processes followed for the utilization of an Active Directory platform and the information being collected/ utilized within WINAD for use in the Department's I&A processes.

5. Use of information

- (a) What is/are the intended use(s) for the information?

The intended uses for the information are User Identification, Authentication and Authorization. This information is also used for contacts in the DOS email Global Address List (GAL) and Skype/Lync-C platforms.

- (b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes.

- (c) Does the system analyze the information stored in it? Yes No

If yes:

- (1) What types of methods are used to analyze the information?

[Click here to enter text.](#)

- (2) Does the analysis result in new information?

[Click here to enter text.](#)

- (3) Will the new information be placed in the individual's record? Yes No

- (4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

Yes No

6. Sharing of Information

- (a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Internal Sharing:

WINAD makes its information available via Exchange to Outlook in the form of the Global Address List (GAL).

WINAD also synchronizes this information to the O365 and Microsoft Azure Government (MAG) Azure AD (AAD) tenants.

WINAD's business identity data is shared with any application on OpenNet that requires it for official purposes. All applications that use WINAD can pull the business identity information stored in WINAD and use it within that application.

WINAD makes its information available to Skype-for-Business in a similar format to Exchange and Outlook in the form of the GAL.

The WINAD OpenNet GAL information is synchronized with the DOS Public Affairs Communicating Electronically (PACE) network's Active Directory and vice/versa.

External Sharing:

The WINAD OpenNet GAL information is synchronized with the USAID network's Active Directory and vice/versa.

(b) What information will be shared?

GAL - name, work phone, work address, business email, company, department, office and photo, if it was added to AD

MAG and O365 Azure ADs – all information in the GAL (see above)

Any application on OpenNet (including Skype) –all information in the GAL (see above)

PACE and USAID - all information in the GAL (see above)

(c) What is the purpose for sharing the information?

Internal:

GAL – so users can lookup business contact information of other users for communication purposes.

O365 and MAG Azure ADs – see above for GAL, as well as for identification, authentication, authorization, and auditing of application activity.

Any application on OpenNet (including Skype) – see above for both GAL and O365 Azure AD.

PACE and USAID – OpenNet GAL information is shared for the purpose of allowing OpenNet, PACE and USAID users to communicate with each other.

(d) The information to be shared is transmitted or disclosed by what methods?

The information WINAD shares with each system is transmitted electronically through appropriate network infrastructure, various Active Directory tools or services such as the Lightweight Directory Access Protocol (LDAP, default port 389) or Secure LDAP (LDAPS, default port 636).

- (e) What safeguards are in place for each internal or external sharing arrangement?

External:

Data is only shared with PACE and USAID through encrypted LDAPS transmissions.

Internal:

Department of State information systems (e.g., applications, servers, etc.) run queries to the WINAD Database(s) utilizing the LDAP and/or LDAPS functionality described in 6 (d) or similar network based communication method through OpenNet. This ensures only secure, authorized network based transactions occur, which is a native function to Microsoft's AD product.

- (f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

The primary privacy concern that was identified was that personal information could be stored in WINAD, and subsequently shared with all users and systems receiving access to WINAD's information. The concern was addressed by keeping the type of information collected to business information (e.g., name, business phone number, business email address, business physical address). The encrypted LDAP transmissions is another safeguard employed to protect data during transmission.

7. Redress and Notification

- (a) What procedures allow individuals to gain access to their information?

Users can open Outlook and look themselves up in the GAL. Any changes made in the GAL, such as through myProfile, will be reflected in any other system that uses the GAL provided by WINAD.

- (b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes No

If yes, explain the procedures.

Users can update their Active Directory information by sending an incident request to IT Service Center. Users can also update their information themselves through the myProfile website <https://myprofile.a.state.sbu/>

If no, explain why not.

- (c) By what means are individuals notified of the procedures to correct their information?

OpenNet users are notified via myProfile to update or correct their information every 90 days as needed. Users are informed when onboarding to contact ITSC for all of their IT needs, which includes sending requests for changing AD/GAL information.

8. Security Controls

- (a) How is the information in the system secured?

The information in the system is secured by Data at Rest encryption (DAR). All servers are secured using DOS security configuration guides. Administrative access to the information within the system is enforced through Rule Based Access Controls (RBAC).

- (b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

Administrative rights to WINAD’s Active Directory are controlled and limited through rights delegation which includes least privilege and separation of duties amongst the administrators. The network firewalls protect WINAD’s Active Directory from access outside the OpenNet network and the Microsoft cloud firewalls protect the data synchronized to the DOS instances of Azure Active Directory.

- (c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

A product called Change Auditor for Active Directory audits changes in real-time to the data in WINAD. Change Auditor looks for changes to all WINAD data (e.g., if a password is changed, then Change Auditor will capture the event surrounding the password change).

- (d) Explain the privacy training provided to authorized users of the system.

All OpenNet users are required to attend security training conducted by Diplomatic Security the first time users are granted access to OpenNet. Afterwards, there are annual on-line security training refresher courses, covering OpenNet security policies and practices, and the basic rules of behavior. Privacy is part of the training syllabus. All Department of State employees are required to complete the mandatory FSI online training course, PS800, Cybersecurity Awareness, which includes a module on privacy. All civil service, foreign service and locally employed staff that handle PII are required to complete the FSI course, PA459, Protecting Personally Identifiable Information.

- (e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? Yes No
If yes, please explain.

WINAD is the authentication system for OpenNet applications. To use WINAD and its data or its dependent applications and the data they collected from WINAD, users must authenticate to WINAD first. Users authenticate to workstations on OpenNet via Smartcard authentication. Global OpenNet uses an AD provided username/password and an additional RSA Secure ID authentication mechanism. WINAD supports encrypted and unencrypted LDAP data queries and the AD database itself is encrypted.

O365 Azure AD is the authentication system for O365 and other applications configured to utilize O365 Azure AD. Use of O365 Azure AD and its data or its dependent applications and the data they collected from O365 Azure AD first requires authentication to O365 Azure AD. For users on OpenNet or remote users using Global OpenNet, authentication to WINAD is trusted by O365 Azure AD, so the same controls in place for WINAD apply to O365 Azure AD. For remote users accessing O365 Azure AD without Global OpenNet, authentication requires either smartcard logon or username/password and an additional O365 Azure AD MFA authentication. All data retrieved through O365 Azure AD uses SSL encryption.

WINAD Administrative Users are also approved business users. However, their Administrative rights to WINAD are controlled and limited through rights delegation which includes least privilege and separation of duties amongst all of the administrators.

(f) How were the security measures above influenced by the type of information collected?

The security measures for WINAD were influenced by the role authentication plays in protecting Department of State data. Authentication is the first major access control to nearly all Department of State data, including the identity and authentication information contained within WINAD.

9. Data Access

(a) Who has access to data in the system?

All authenticated users have access to the GAL and the business identity information contained in the GAL.

(b) How is access to data in the system determined?

All authenticated users have access to the GAL which displays the information collected as described in Sections 3(d) and 6(a) above. Users become authenticated when they obtain an OpenNet account after onboarding at Department of State; see procedures already described above in Section 4(h).

Administrative access to the data in WINAD is only granted to Department of State government employees and contractors who have an approved business justification for requiring access [as described in 9 (a)]. These individuals are given least privilege and functionality to perform the required business function.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? Yes No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

All users (both regular and privileged) have read access to all data in the GAL, and most LDAP data in the WINAD database (DB). WINAD system administrators have write access to portions of the WINAD DB based on their role (e.g., Paris System Administrators can only manage Paris users).

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

All authenticated OpenNet users, administrators, and applications have read access to the GAL and LDAP data in WINAD. Authenticated administrators have write access to portions of the WINAD database based on their role (e.g., Paris System Administrators can only manage Paris users). The Change Auditor tool is used as an auditing tool for WINAD (iMatrix 633) for the purpose of detecting changes done by authenticated administrators in the Active Directory Enterprise environment.

In order to facilitate communication, the information in the GAL must be available to all authenticated OpenNet users, administrators, and applications. Users and administrators are guided by their privacy training to use the GAL information appropriately for business purposes.