Privacy Impact Assessment
for the

Application Authentication System (AppAuth)

DHS/ALL/PIA-060

February 27, 2017

Contact Point
Stephen Pyfrom
AppAuth System Owner
Information Sharing Environment Office (IS^2O)
Office of the Chief Information Officer
(202) 447-5647

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Application Authentication System (AppAuth) is a Department of Homeland Security (DHS) enterprise system developed and operated by the DHS Headquarters Information Sharing and Services Office (IS^{2}O). AppAuth is a DHS single sign-on enterprise authentication service,[1] which provides a uniform authentication service based on Microsoft's Active Directory services. DHS is publishing this Privacy Impact Assessment (PIA) because AppAuth accesses and uses personally identifiable information (PII) within the component active directory environments to adequately leverage authentication across DHS.

Overview

The Application Authentication System (AppAuth) was developed by the Department of Homeland Security (DHS) Headquarters Information Sharing and Services Office (IS^{2}O) to support its mission to deliver the services required by the DHS enterprise for mission, business management, and information technology support. AppAuth enables DHS users across the Department to log on to enterprise applications using their normal component login credentials. The system provides basic authorization services[2] via security groups that can be established within an organization and used as the basis for internal authorization logic to determine level of access for an individual user.

AppAuth provides cross-domain authentication[3] of DHS users for the purposes of using DHS enterprise applications via two-way trusts.[4] In a two-way "forest"[5] trust relationship, AppAuth will trust a component's active directory at the forest level[6] and a component's active directory will trust AppAuth. The forest allows separate active directory forests to exchange information with other environments while still allowing each component active directory forest to maintain complete control over its own forest. In this model, AppAuth is the trusted domain; AppAuth allows DHS Component end users to use their current component credentials to access DHS applications hosted within the AppAuth forest. In this role, AppAuth is the "container"[7] for

[1] Authentication is the process or action of verifying the identity of a user or process. Credentials that a user provides are compared to those on file. If the credentials match, the user is granted authorization for access.
[2] Authorization is the function of specifying access rights to individual users or resources.
[3] Cross-domain authentication gives users the ability to log in to their enterprise applications from their component workstation.
[4] A two-way trust is an active directory authentication connection between two DHS Components such as Headquarters and the Federal Emergency Management Agency (FEMA).
[5] A forest is a directory that houses all users' objects in their environment. These objects allow users to log on to their workstation.
[6] A forest level is the directory operating system level such as Windows 2008 level or Windows 2012 level.
[7] AppAuth acts as a "container" or repository of active directory attributes/server assets for the purposes of providing Single Sign-On (SSO) capability to enterprise applications. AppAuth is not the primary source of these attributes, but collects the attributes required by the DHS Components to implement the functionality.

those enterprise applications that have subscribed to the Single Sign-On (SSO) service based on Windows Integrated Authentication (WIA), which is based on Kerberos.[8]

The two-way forest trust between AppAuth and DHS Components will ensure that Components have a centrally-controlled, robust authentication capability for accessing their enterprise applications infrastructure and services. Component domains hold end user credentials but leverage AppAuth. This includes support for Data Center-provided as a service applications (e.g., SharePoint as a Service, Work Place, and Customer Relationship Management as a service). These trusts are essential to the assurance that only authorized users are able to leverage AppAuth verification of credentials. These credentials are leveraged at a system level and are not directly accessed by end users. There is no direct input of PII or solicitation of PII from an end user. AppAuth itself, via approved trusts, ingests this information from already established identity stores from DHS Components. The AppAuth Active Directory is populated via already gathered data from an existing DHS Active Directory. These credentials are input and controlled via the component's active directory by privileged users (system administrators). The PII that is collected, is in the form of Human Resource Information Technology (HRIT), which contains basic attributes about the user account. These include name, user account, duty locations, phone numbers, work email addresses, and other non-sensitive identifiers. This data is used primarily for the purposes of identifying users and organizing user communities. The PII is not extracted or used for any particular portable service, but is used for identification purposes. The PII is maintained in AppAuth Active Directory as long as the account is active.

AppAuth has established trusts with DHS Component Active Directory domains such that users' home domain credentials can be accepted for access to shared information. Component active directory systems contain PII.

AppAuth has many benefits, especially those that minimize privacy risks. AppAuth provides the below benefits for all DHS Components:

- Mitigates risk for access to 3rd-party sites (user passwords not stored or managed externally);
- Reduces password fatigue;[9]
- Reduces time spent re-entering passwords for the same identity; and
- Reduces IT costs due to lower number of IT help desk calls about passwords.

[8] The Kerberos version 5 authentication protocol provides a mechanism for authentication - and mutual authentication - between a client and a server, or between one server and another server.
[9] Password fatigue is experienced when an individual is required to remember an excessive number of passwords as part of his or her daily routine.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The Secretary of Homeland Security is charged with taking reasonable steps to ensure that the Department's information systems and databases are compatible with each other and with appropriate databases of other departments and agencies.[10] In fulfilling these responsibilities, the Secretary exercises direction, control, and authority over the entire Department, and all functions of all Departmental officials are vested in the Secretary. AppAuth is consistent with and promotes carrying out these responsibilities.

Relevant legislative and policy authorities for AppAuth include the following:

- Federal Information Security Modernization Act of 2014 (Pub. L. 113-283);
- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," revised, July 26, 2016;
- DHS Management Directive MD 140-01, "Information Technology Systems Security," July 31, 2007;
- National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006; and
- NIST Special Publications (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.

Additional programmatic authorities may apply to maintenance of the credential.

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

Information in AppAuth is covered by the DHS/ALL-037 E-Authentication Records System of Records Notice (SORN).[11] The purpose of this system of records is to collect information in order to authenticate an individual's identity for the purpose of obtaining a credential to electronically access a DHS program or application.

[10] The Homeland Security Act of 2002, Pub. L. 107-296, codified at 6 U.S.C. § 112 (2012).
[11] *See* DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014), *available at* https://www.gpo.gov/fdsys/pkg/FR-2014-08-11/html/2014-18703.htm.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

An Authority to Operate (ATO) was granted for AppAuth in January 2014. A new ATO will be granted upon completion of this PIA.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. AppAuth follows from General Records Schedule 3.2 and DHS Data Retention policies, keeping audit records for 90 days online before shipping the electronic logs off to offsite storage for 7 years. All user information is kept for 6 years following the deletion of the account. Online information is removed once a user is removed from a component identity store or directly from the AppAuth domain.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No. The provisions of the Paperwork Reduction Act are not applicable to AppAuth because AppAuth does not collect information from members of the public. Only information from DHS personnel is collected.

Section 2.0 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.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

AppAuth collects a subset of information from active directories on DHS employees and contractors to provide a uniform authentication service. This information is collected when accounts are created from the already existing identity stores. When a user is onboarded, his or her human resource information[12] is solicited by personnel security and provided to be passed on for insertion into the DHS Active Directory. Privileged account information is solicited via Privileged Access Requests (PAR). AppAuth uses the following data elements:

- Full Name

[12] The collection of this information is described in DHS/ALL/PIA-043 DHS Hiring and Onboarding Process (April 22, 2013), *available at* https://www.dhs.gov/publication/dhs-hiring-and-boarding-process-dhsallpia-043.

- Work Phone Number
- Work Location (Component/Directorate Office)
- Work Address
- Work Email Address

2.2 What are the sources of the information and how is the information collected for the project?

AppAuth information comes from DHS Component data stores within trusted active directory domains. This information has already been collected when an employee has onboarded to DHS and his or her information is entered into the active directory. The information AppAuth uses is not collected directly from the individuals, but rather from the trusted component active directory domains. The information is transmitted via two-way trust, allowing for the exchange of active directory data for users and systems across DHS and component user/system communities. User attributes locally contained within a component active directory can now be synced across the forests to allow for activities across the DHS enterprise via AppAuth. This information is not accessible and cannot be solicited by end users as this transfer of information is system-to-system (e.g., CBP's Active Directory to AppAuth).

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

No. AppAuth is a completely internalized DHS system that does not leverage third-party publicly available repositories.

2.4 Discuss how accuracy of the data is ensured.

The accuracy of the data is the responsibility of the component administrators who provide the information through their own active directories, which is where AppAuth pulls the information. Those component administrators are responsible for maintaining the accuracy of their own active directory data stores. Any changes made to their local component domain instances will propagate to AppAuth via active directory users and systems dashboards as well as supporting systems that leverage the AppAuth identity user/systems stores. Because AppAuth transactions do not modify information in transit or at rest, the data remains unchanged as it is stored in the component location. AppAuth leverages Kerberos,[13] which is a widely used protocol used for the authorization/authentication used with the SSO functionality. Kerberos uses key-based security to

[13] The Kerberos version 5 authentication protocol provides a mechanism for authentication - and mutual authentication - between a client and a server, or between one server and another server.

ensure the confidentiality and integrity of authentication credentials and attributes in transit and at rest.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk to data integrity since AppAuth relies on active directories to continually provide the information. This may create data inaccuracies if the active directory data passed to AppAuth is not regularly refreshed.

Mitigation: The accuracy of the data is the responsibility of the component administrators who provide the information through their own active directories. AppAuth pulls the information from those active directories. All changes made in those active directories are synced automatically in AppAuth when they are made in the active directories. Changes across the local domain occur in a near instantaneous manner.

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

AppAuth uses non-sensitive PII for the unique identification of DHS employees and contractors. No Sensitive PII is collected, transmitted, or stored as a result of these services/capabilities. Because a number of systems leverage AppAuth as well as the underlying component identity stores, those applications can leverage a number of directory lookup services. For example, Microsoft Exchange and SharePoint use AppAuth to grant a user access to his or her email or SharePoint sites without going through a login step. These applications do not individually store this information, but query the information stored in a component or AppAuth Active Directory.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

No.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes, each DHS Component administrator has authority over his or her active directory identity stores. Administrators are responsible for the maintenance and management of their DHS

user communities within those repositories to ensure the accuracy and validity of those stores. That information is replicated to AppAuth via the approved two-way forest trust.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that the information within AppAuth will be used for a different purpose than for which it was intended.

Mitigation: Only a small group of DHS system administrators have access to view or modify user data within AppAuth. All AppAuth users are trained in annual DHS Privacy training prior to being granted AppAuth credentials. These system administrators require more a robust background investigation and subsequent training before gaining administrative access to AppAuth. Individuals do not have direct access to modify, insert, or retrieve PII data. Due to the nature of the information in AppAuth, the risk of using this information in a manner that would cause harm to the individual is low.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

AppAuth does not provide notice prior to collection of information because it does not collect information directly from individuals. Further, it is difficult to provide notice to individuals that their information will be used by AppAuth since there is no user interface. DHS is providing notice about AppAuth through this PIA. As described above, AppAuth does not collect information directly from individuals, but instead relies upon information collected by the Office of Personnel Management (OPM) and DHS during the personnel onboarding processes. This information is covered by existing OPM and DHS SORNs, and Privacy Act Statements are provided at the point of information collection.

The information collected during the onboarding process is now being maintained for the new use in AppAuth. The maintenance of this information is covered under the existing E-Authentication Records System of Records.[14] The purpose of this system is to collect and maintain information in order to authenticate an individual's identity for the purpose of obtaining a credential to electronically access a DHS program or application.

[14] *See* DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014), *available at* https://www.gpo.gov/fdsys/pkg/FR-2014-08-11/html/2014-18703.htm.

This PIA serves as additional notice that information collected during the onboarding process is used for the AppAuth enterprise authentication service.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

AppAuth does not directly solicit information from individuals. Therefore, individuals cannot consent to or opt out of providing information to AppAuth. This information is pulled directly from existing information provided by individuals during their onboarding processes. Most of the information, such as work email and work phone number, are provided by the Department to the individual.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: Individuals may not be aware that their information is being used by AppAuth and do not have an opportunity to consent prior to its use.

Mitigation: DHS provides employees with notice, and employees consent to general uses of their information, when they submit their biographic attributes to DHS upon the onboarding process. Privacy Act Statements are provided at the time of collection and have published SORNs to further provide notice. This PIA serves as additional notice that information collected during the onboarding process is used by AppAuth to provide individuals with the ability to log on to enterprise applications using their normal component login credentials.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The AppAuth system leverages the credentials of component-maintained active directory identity stores. As a result, once components make changes or deletions from their active directory, the online record will be removed from within AppAuth. However, AppAuth maintains daily backups of activity directory databases which allows for the rollback of changes, recovery from disaster, or response to incidents. As a result, AppAuth subscribes to the DHS Data Retention Policy requiring the retention of data for no less than 7 years. This information is encrypted and stored at an offsite location. This retention schedule is less than the retention period for the original collection of data during the onboarding process.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a risk that information will be retained for longer than is required or needed in AppAuth.

Mitigation: This risk is mitigated. AppAuth has a retention schedule that is shorter than the retention period for the original collection for during the onboarding process. Because AppAuth maintains daily backups of activity directory databases, it will always have the most current information for employees and contractors. AppAuth follows DHS Data Retention policies by keeping audit records for 90 days online before shipping the logs off to offsite storage for 7 years. All user information is kept for 6 years following the deletion of the account.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

No, AppAuth does not share data outside of the Department.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

AppAuth does not share data outside of the Department.

6.3 Does the project place limitations on re-dissemination?

AppAuth is not a primary source for the individual PII data. The data originates with the DHS Component that can re-disseminate information as stated in the original SORNs that cover the collection of the information during the onboarding process. AppAuth does not disseminate data outside the Department.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

AppAuth does not make any disclosures outside of the Department.

6.5 Privacy Impact Analysis: Related to Information Sharing

There are no privacy risks to external information sharing because AppAuth does not share information outside the Department.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

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

Individuals do not have direct access to AppAuth information as authorization is a system-to-system transaction. Any update of information is performed at the component active directory authorization boundary. Employees may update their component active directory information by contacting the component's Help Desk.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Procedures to allow for the corrections of inaccurate or erroneous information would take place at the component active directory level. The information in AppAuth would be updated as a result of the changes to the component active directory. Employees and contractors may update their component active directory by contacting the component's Help Desk.

7.3 How does the project notify individuals about the procedures for correcting their information?

Because the information in AppAuth is the information as the data in the active directory databases, notification to individuals of the procedures for correcting data in AppAuth is the same as that of the component active directory databases or the source systems that contain the information collected during the onboarding process.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that an individual will not be able to receive appropriate access, correction, and redress regarding AppAuth's use of PII.

Mitigation: This risk is partially mitigated because users cannot directly update their information in AppAuth. However, AppAuth has a near immediate refresh from the component active directory databases. AppAuth is dependent on the component active directory database administrators and the source system owners of the information collected during the onboarding process to input the correct information about individuals. However, since the information used in AppAuth is the same as that from the component active directory databases and the source system information collected during the onboarding process, individuals should follow redress procedures for these.

Section 8.0 Auditing and Accountability

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

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

AppAuth maintains a detailed auditing functionality for all users and user activities within the information system. This information is readily monitored by systems administrators, security officials, and the DHS Security Operations Center (SOC). A full listing of auditable events for the information system is available via the AppAuth approved System Security Plan. This describes audit capability, responsibility, and requirements in detail. This auditing includes: the action being performed, the user object performing the action, SUCCESS/FAIL of the event, and the timestamp. Information is monitored and processed via automated auditing services for review by the DHS SOC for identification of potential malicious activity. All activities identified as malicious are available via the AppAuth Systems Security Plan.

AppAuth ensures that all systems administrators and privileged users with access to the system have undergone annual privacy training, systems administrator training, and Privileged User training to ensure awareness of all system and privacy requirements.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

DHS provides the required privacy and security awareness training to all employees and contractors, which equips them with information on safeguarding PII. The only "users" who will have access to AppAuth will be the system administrators, who are considered privileged users, and require more robust background investigation and subsequent training before gaining administrative access to any sensitive systems. All AppAuth system administrators are required to take DHS IT Security Awareness Training. DHS Privacy Training, Privileged User Training, and Role-Based Systems Administrator Training via the DHS HQ Training Site. System administrators are determined by the system owner for purposes of supporting the information system. All administrators are approved by the system owner and information systems security officer prior to being granted access to the information system. Non-administrative users do not have access to the information system.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

AppAuth provides only for system-to-system interfaces. Therefore, aside from system administrators, there are no users of AppAuth.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

There are no external MOUs in place because AppAuth does not share information. However, if the need arises, DHS Headquarters IS^{2}O will enter into MOUs as appropriate, and include the necessary level of review through all stakeholders, including the DHS Privacy Office.

AppAuth is governed by the Enterprise System Security Agreement (ESSA). Version 2.0 is active and signed by all DHS Component CISOs. The ESSA is an authoritative document which defines the relationships between DHS Component identity stores and AppAuth. This specifically details system architecture, security requirements, current security posture, and platform/tenant responsibilities. All other agreements are identified and maintained via Department-approved Interconnection Security Agreement between parties.

Responsible Officials

Stephen Pyfrom
AppAuth System Owner
Information Sharing Environment Office (IS^{2}O)
Office of the Chief Information Officer

Approval Signature

Original, signed version on file at the DHS Privacy Office

_____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security