Privacy Impact Assessment
for the

DHS Access Lifecycle Management

DHS/ALL/PIA-058

January 24, 2017

Contact Point
Thomas McCarty
Identity Services Branch
Information Sharing and Services Office (IS2O)
Office of the Chief Information Officer
(202) 447-3729

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

Abstract

The Department of Homeland Security (DHS) Access Lifecycle Management (ALM) is the technology and business process that manages the identities and access rights of DHS employees and contractors, ensuring that they only have access to approved systems and applications. DHS is publishing this Privacy Impact Assessment (PIA) because ALM uses, stores, and disseminates personally identifiable information (PII) of DHS employees and contractors in order to manage their accounts and identities.

Overview

The purpose of the DHS Headquarters (HQ) Office of the Chief Information Officer (OCIO) Information Sharing and Services Office (IS2O) Identity Services Branch is to ensure that the DHS workforce has appropriate access to the protected data, facilities, systems, and applications that they need to perform their mission. The Identity Services Branch created the ALM technology to automate and streamline the many business processes currently in place to centralize and manage identity-based access rights for DHS employees and contractors.

Current DHS employees often take on new job functions that require access to different systems. ALM manages the user's digital identity, which includes his or her attributes, access rights, and the policies that apply to him or her. ALM then ties the user's digital identity to his or her credential, which at DHS is the Personal Identity Verification (PIV) card. This allows the user to authenticate log-on access to applications.

Before a new employee onboards, ALM receives core identity information about a newly active employee from the Trusted Identity Exchange (TIE),[1] and uses digital policies to automatically provide the new employee's account access and authorization information to the network, email, facility control, training, and time and attendance systems. This automation eliminates most of the human-to-system interaction with identity data and significantly reduces the risk of unintentional disclosure of privacy-sensitive information, while increasing user productivity.

As this process suggests, ALM stores user information in its secure repository, including:

- **Identity attributes**. Attributes that describe a person, such as name, location, phone number, email, department, and division (for complete list, see Section 2.0 Characterization of the Information); and

---

[1] *See* DHS/ALL/PIA-050 DHS Trusted Identity Exchange (TIE), *available at* www.dhs.gov/privacy.

- **Account attributes**. Attributes associated with specific user accounts that are required by the application, such as for log in purposes (e.g., usernames), and entitlements (e.g., read only, view report) dictating what the user can do within the application.

After ALM creates a user's digital identity and grants his or her access to DHS systems as part of the onboarding process, the ALM tool supports the entire access lifecycle for the user. When DHS employees and/or contractors require new access rights because of a change in position or responsibilities, they can request additional access through an easy-to-use ALM online self-service portal. Each request undergoes an automatic validation process to make sure that it does not violate policies or present other conflicts (e.g., Separation of Duties (SoD) violations[2]). The request is then routed to the employee's manager or the contractor's Contracting Officer's Representative (COR), and if necessary, to the application owner (according to the specific built-in workflows for specific applications). If the manager or COR approves the request, ALM automatically grants the user with access and notifies the user via email of the status. This process eliminates the need to use paper forms, email, or fax in order to submit an access request.

ALM ensures that users do not use unapproved channels to get access to applications, systems, or facilities they do not need, monitoring such activity and ensuring that inappropriate or unnecessary access is promptly removed. User access to DHS systems is aggregated by ALM periodically to a central view of a user's identity. Any unapproved access can be flagged. In addition, all access is certified at least annually by the system owner and/or the user's manager to review and secure the access on an ongoing basis.

Finally, when a user leaves the organization, the centralized ALM tool streamlines and automates the disabling of his or her accounts and removes his or her access to all systems. This means that no access to systems remains after a user leaves, mitigating the risk of unauthorized, and continued use of the account. Table 1 describes the ALM use cases in more detail.

<div align="center">Table 1: ALM Use Cases</div>

Use Case	Description
User Onboarding	ALM provides new employees and contractors with a single digital identity and any access they require on their first day via automatic provisioning. This includes any digital forms or approvals necessary along the way.
Access Request	ALM offers users an easy-to-use self-service portal for requesting additional access. The tool has automated workflows in place to route requests to system owners and supervisors for approving or rejecting such requests. It then automatically grants access if it is approved, or notifies users by email if the request is rejected.

---

[2] SoD violations occur when a user requests or is granted access that forms a conflict of interest combination, which should not be possessed by a single user (e.g., Accounts Payable and Account Receivable).

Use Case	Description
Access Certification	ALM periodically initiates a review of user access rights to make sure that users still need their current level of access for their job functions. Designated reviewers receive a notification that allows them to approve or revoke a user's access rights.
Enforcement of Separation of Duties (SoD)	SoD violations occur when a user requests or is granted access that forms a conflict of interest combination, which should not be possessed by a single user (e.g., Accounts Payable and Account Receivable). ALM can detect and remove existing conflict of interest combinations of access and can proactively prevent new ones from occurring during the access request process. It can also prevent them from occurring during the access request process.
Access Reconciliation	ALM uses built-in workflows to identify, reverse, or remove changes that are made to accounts (e.g., creation, modification, deletion) without going through the proper access request and approval process.
User Off-boarding	ALM allows access across all systems to be quickly removed using automated de-provisioning workflows when employees or contractors leave the organization.
Analytics and Reporting	ALM provides robust analytics and reporting capabilities. For example, it can generate detailed reports of all identities that have access to a specific system, and all the access rights that a given identity holds.

The scope of ALM is limited to internal DHS identity, credential, and access management (ICAM) data [3]. ALM applies to the Sensitive but Unclassified (SBU) security domain, and is not scoped directly to serve National Security Systems on the classified domains (i.e., "high side" applications). This also means that ALM does not directly share DHS ICAM data with non-DHS (external) systems.

ALM is a critical component to support important DHS employee and productivity initiatives, including the TIE, Attribute-Based Access Control (ABAC), PIV Smart Cards, SSO, Mobile Authentication, and the DHS Continuous Diagnostics and Mitigation (CDM) Program[4]. The following describes how ALM will impact each initiative.

Trusted Identity Exchange (TIE)[5]

The TIE is a secure DHS exchange service; it serves as an intermediary between

---

[3] For the purposes of this PIA, "DHS ICAM data" encompasses both person- and machine-identities. A person's digital identity contains information attributed to a human. Machine (or non-person) identities contain information about "things," such as a computer serial number or unique network address—essentially digital attributes that can be used to uniquely identify machines, computer processes, or other "non-person" things.

[4] DHS/NPPD/PIA-030 Continuous Diagnostics and Mitigation (CDM) www.dhs.gov/privacy.

[5] For more information on the TIE, *see* DHS/ALL/PIA-050 DHS Trusted Identity Exchange, *available at* www.dhs.gov/privacy.

authoritative data sources (i.e., systems or applications that maintain information about DHS employees and contractors) and consuming applications (i.e., applications or systems that request information from the TIE about specific DHS employees or contractors). The TIE establishes a consolidated list of identity and access attributes from sources including National Finance Center (NFC) and Integrated Security Management System (ISMS).[6] The TIE allows the consuming applications to leverage existing DHS employee identity attributes to make confident, secure, and effective business and access decisions in a manner that enhances privacy.

The TIE provides a consolidated view of an identity across multiple systems; ALM consumes this data as the basis of identities. Therefore, the TIE acts as a data source for ALM. DHS ALM is a consumer of the TIE and also supports the TIE by ensuring the integrity of the user and identity attributes in the TIE through periodic validation of user accounts and entitlements via access certifications over a secure encrypted channel; certification frequency is determined in consultation with individual system owners and their requirements. This increases the level of confidence in the attributes being used for authorization decisions at the Department.

Fine-Grain Authorization

Today, most IT systems make and enforce user access decisions based on static information provided during the initial provisioning process. A user's level of access tends to remain the same in a given system because most systems do not have automated procedures in place to "re-certify" a user's continued need for a certain level of access. Fine-grain authorization[7] (which can materialize as ABAC) describes an IT system's ability to make a final access determination based on near real-time information from authoritative identity sources.

ALM sets the foundation for fine-grain authorization by ensuring the proper management of identities in the TIE. The TIE, in turn, provides a single interface for consuming applications to request the information required to make dynamic access decision.

Personal Identity Verification (PIV) Smart Cards

Federal employees and contractors are issued PIV smart cards, which are secure credentials that are required to access federally-managed facilities and information systems. In order for a user to use a PIV card to log-on to the DHS network,[8] data about the PIV card must be provisioned to Active Directory (AD). ALM accomplishes this by correlating the user's PIV card to his or her network account, which includes all of his or her access rights. This allows DHS employees and

---

[6] DHS/ALL/PIA-038(b) Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.
[7] Fine-grain authorization is in a planning stage. The effort is part of the Data Framework. The Data Framework PIA, DHS/ALL/PIA-046(b) DHS Data Framework, is available at www.dhs.gov/privacy
[8] PIV authentication to the network is not composed of a system, but is rather configurations to the DHS network. The PIA for the system that issues PIV smart cards is DHS/ALL/PIA-014 Personal Identity Verification, and is available at www.dhs.gov/privacy.

contractors to receive their PIV card and network access on their start date.

Single Sign-On (SSO)

SSO[9] provides a foundation for safeguarding the DHS network and the information stakeholders generate or consume on a regular basis. Furthermore, SSO enhances a user's PIV log-on experience by enabling "one-click" access to applications, following the use of a PIV card to log-on to the DHS network. This reduces the number of passwords that a user has to remember and provides authentication of the user's identity (i.e., proof that the person is who he says he is).

ALM swiftly establishes user accounts to applications prior to access, thereby supporting SSO to only approved functions and accounts.

Mobile Authentication

The Mobile Authentication[10] initiative seeks to bring greater flexibility to the Department by allowing users to access Department information and applications on their government-issued mobile devices wherever and whenever necessary while maintaining a great level of security. Mobile Authentication relies on the identification mechanisms already in place to identify the user and to verify what Department resources he or she is authorized to access. ALM's role is to associate a given mobile device with a person's identity, maintaining it in the same way it maintains other credentials held by the user. This, in turn, enables multi-factor authentication using the mobile device and a centralized method for provisioning and de-provisioning mobile devices.

DHS Continuous Diagnostics and Mitigation (CDM) Program

The CDM program[11] seeks to fortify the security of federal computer networks and systems by providing continuous monitoring, diagnosis, and mitigation activities and tools. It provides network administrators with dashboards to consistently monitor the state of their respective networks, and to swiftly identify and prioritize any threats that require resolution. DHS has been charged with overseeing the deployment of the necessary CDM diagnostic tools across participating federal agencies. DHS is also a user of CDM tools.

ALM supports DHS's implementation of the CDM program by allowing administrators and other officials to see what access rights individual users have throughout their DHS careers. These capabilities include access reconciliation, access recertification, and the enforcement of SoD. The tool detects, assesses, and reduces key risks while decreasing audit and operational costs

---

[9] SSO is in production and is being implemented through multiple service providers at DHS. These systems include CBP ICAM ((CBP-06704-GSS-06704) and DHS Active Directory Federation Services (ADFS): DHS/ALL/PIA-012(b) - E-Mail Secure Gateway (February 25, 2013), available at www.dhs.gov/privacy.

[10] Mobile Authentication is currently in development.

[11] The CDM Program is an ongoing effort being developed by DHS. For more information, see http://www.dhs.gov/cdm. DHS/NPPD/PIA-030 Continuous Diagnostics and Mitigation, *available at* www.dhs.gov/privacy.

by continuously monitoring for policy violations and security threats. It provides essential security status information to allow for the remediation of any violations. ALM's continuous monitoring of access can keep the environment secure and feeds directly into DHS's implementation of CDM tools, which aim to efficiently allocate cybersecurity resources and provide adequate, risk-based, and cost-effective cybersecurity.

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?

Relevant legislative and policy authorities for ALM include the following:

Primary Authorities

- OMB Memorandum M-15-01: Guidance on Improving Federal Information Security and Privacy Management Practices (October 3, 2014);
- Federal Information Security Modernization Act of 2014 (P.L. 113-283);
- OMB Memorandum M-14-03: Enhancing the Security of Federal Information and Information Systems (November 18, 2013);
- Federal CIO Council, United States Government Concept of Operations for Information Security Continuous Monitoring (October 2013);
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors (February 3, 2011);
- OMB Memorandum M-05-24: Implementation of HSPD-12 Policy for a Common Identification Standard for Federal Employees and Contractors (August 5, 2005); and
- OMB Memorandum: Streamlining Authentication and Identity Management within the Federal Government (July 3, 2003).

Secondary Authorities

- OMB Memorandum M-17-05: Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements (November 4, 2016);
- Executive Order 13741, Amending EO 13467 to Establish the Roles and Responsibilities of the National Background Investigations Bureau and Related Matters (September 29, 2016);
- OMB Circular No. A-130, Managing Information as a Strategic Resource (July 27, 2016);
- OMB Memorandum M-16-04: Cybersecurity Strategy and Implementation Plan

(CSIP) for the Federal Civilian Government (October 30, 2015);

- Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (October 7, 2011);

- National Institute of Standards and Technology (NIST), U.S. Department of Commerce, NIST Special Publication 800-137, Information Security Continuous (ISCM) for Federal Information Systems and Organizations (September 2011);

- Executive Order 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information (June 30, 2008);

- OMB Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007); and

- OMB Memorandum M-06-18: Acquisition of Products and Services for Implementation of HSPD-12 (June 30, 2006);

- OMB Memorandum M-06-16: Protection of Sensitive Agency Information (June 23, 2006);

- OMB Memorandum M-00-10: Procedures and Guidance on Implementing Government Paperwork Elimination Act (April 25, 2000).

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

ALM receives SORN coverage under the DHS/ALL-037 E-Authentication Records System of Records[12] System of Records Notice (SORN). This SORN allows DHS to collect, maintain, and retrieve records about individuals who electronically authenticate their identities.

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

ALM functionality is currently fully operational at DHS HQ. The functionlaity will be rolled out in a phased approach, which will include a subset of ALM capabilities for a limited set of users in advance of a Department-wide implementation in FY17. Department-wide roll-out will begin in FY18 through FY21. It will include the ongoing integration of existing applications and services with the ALM tool.

At this time, ALM does not have a system Security Plan (SSP) in place. However, an SSP in full compliance with DHS 4300A Sensitive Systems Handbook[13] will be established in

---

[12] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).
[13] DHS 4300A Sensitive Systems Handbook, available at

anticipation of a final authorization to operate (ATO).

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

Yes, General Records Schedule 3.2, Information Systems Security Records, Item 031, Disposition Authority DAA-GRS-2013-0006-0004[14] (see Section 5 for more detail).

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.

The provisions of the Paperwork Reduction Act are not applicable to ALM because no information is collected directly from the public.

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.

ALM will manage the identities and access rights of all DHS employees and contractors. In order to do this, ALM collects and stores user information, including:

- **Identity attributes**. Attributes that describe a person, such as his or her name, location, phone number, email, department, and division; and

- **Account attributes**. Attributes associated with specific user accounts that are required by the application, such as for log in purposes (e.g., usernames), and entitlements (e.g., read only, view report) dictating what the user can do within the application.

ALM builds an identity for DHS employees and contractors by aggregating attributes gathered from the TIE, a secure DHS attribute exchange service that will provide ALM a view of identity information that exists in various authoritative sources. The TIE establishes connections to internal authoritative data sources and provides a secure, digital interface to internal DHS consuming

---

https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf

[14] General Records Schedule 3.2: Information Systems Security Records, available at
http://www.archives.gov/records-mgmt/grs/grs03-2.pdf

applications.[15] ALM builds a DHS user's identity using these attributes, and uses them to support physical and logical access control within DHS. While additional attributes may be added at a later point (at which point this PIA will be updated accordingly), ALM will collect the following identity attributes:

Attribute	Purpose for Collection
First Name	User-friendly way to identify the person during interactions with the system.
Middle Name	User-friendly way to identify the person during interactions with the system.
Last Name	User-friendly way to identify the person during interactions with the system
City	Identify the location of a person for reporting purposes. User is able to self-assert to update location.
State	Identify the location of a person for reporting purposes. User is able to self-assert to update location.
Country	Identify the location of a person for reporting purposes. User is able to self-assert to update location.
Organization Code	Used for onboarding, off-boarding, and policies based on organization. Also used to assign workgroups for Human Resources functions.
Organization Level 1	Used for identifying the Component in which the user works. Creates identity within the system per Component.
Organization Level 2	Used for reporting purposes and for routing of certain work items to workgroups designated for an organization (OCIO, Office of the Chief Security Officer).
Position Title	Used for the creation of roles for assignment of access.
Email	Used to send communications and notifications.
Employee Type	Used for driving workflows and policies based on employee and contractor access.
Contract Number	Used to associate a contractor with a valid contract and remove access upon completion of contract.
Clearance	Used for policies to dictate initial access request for classified networks.
Entrance on Duty Date	EOD Start date used for provisioning access.
Departure Date	Departure date used for removal of access.
Executive Flag	Used for reporting and communications.

---

[15] DHS/ALL/PIA-050 – DHS Trusted Identity Exchange, available at www.dhs.gov/privacy.

Attribute	Purpose for Collection
Status	Used for tracking active vs. inactive status.
Manager	Supervisor for an employee or contractor that is responsible for approving access decisions.
EDIPI	PIV card unique identifier used for correlation purposes.
Person Handle	ISMS unique identifier, used to uniquely identify users.

Once the attributes are collected and identities created, ALM begins managing the lifecycle of individual identities by onboarding the user, creating his or her accounts, and assigning entitlements to DHS systems integrated with ALM. The process of creating accounts can happen in an automated fashion (e.g., an account is created for a user based on his or her job function), or upon request by the user. When users request access to an application, ALM will either use the information about that user that is already known to create the account, or, if the application being requested requires additional information, an electronic form may be presented to the user to collect additional information. Account attributes depend on the specific application; however, they typically include:

- Account ID;
- Name;
- Email address; and
- Entitlements (this describes the access rights that an individual has to a given application).

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

Generally, ALM does not collect information directly from the user. ALM is a consuming application of the TIE. The TIE is a secure DHS attribute exchange service that will provide ALM a view of DHS employee and contractor identity-related information from various authoritative sources. ALM will then build a user's identity by aggregating this information. If information does not exist in any other DHS system, ALM may collect information directly from users; potential examples include allowing a user to self-assert his or her location and building information. The primary providers of DHS authoritative identity source information for the TIE include:

- **Office of the Chief Security Officer (OCSO) Integrated Security Management System (ISMS)**:[16] The DHS Enterprise source of authority for personnel security information, including suitability, investigation status, and security clearance for all DHS employees

---

[16] DHS/ALL/PIA-038(a) Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.

and contractors across all components;

- **OCSO Identity Management System (IDMS):**[17] The DHS Enterprise source of PIV credential information, including credential identification and biometrics for all DHS employees and contractors, except for the U.S. Coast Guard (USCG) personnel whom are considered a military branch, and, who use Common Access Card (CAC) smart cards, information that resides in a Department of Defense (DoD) system; and

- **Human Capital Business Systems Enterprise Integration Environment (HCSB EIE):** The Human Resources (HR) data warehouse that contains data about DHS federal employees for all DHS Components, except for the U.S. Coast Guard military.

- **DHS Enterprise Directory (also known as AppAuth and Active Directory Lightweight Directory Services (AD LDS)):**[18] The DHS Enterprise Directory operated by the OCIO Enterprise Services Development Office (ESDO) and which contains Active Directory (AD) information for all DHS employees and contractors. ALM receives this information from the TIE after it has been originally collected by these systems. DHS will add any additional sources used by ALM to Appendix A.

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.

2.4 Discuss how accuracy of the data is ensured.

ALM receives information from the TIE, which brokers the information between identity source systems and the ALM system (see Section 2.2). The responsibility for maintaining accurate information lies with the source system. If, however, user information is updated in the source system, that same information is automatically updated in ALM (this typically occurs at least daily). It is ALM's responsibility to ensure this automatic data correction process is functioning properly. In addition ALM provides recertification capabilities, allowing accounts and access to be reviewed quarterly or annually based on risk by a user, manager, or other official to validate that the account information is correct and that the employee or contractor should maintain his or her access to IT systems. TIE continuously overwrites and eliminates data based on updates from underlying authoritative data sources.

---

[17] DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System, *available at* www.dhs.gov/privacy.
[18] DHS/ALL/PIA-012(b) E-Mail Secure Gateway (February 25, 2013), *available at* www.dhs.gov/privacy.

2.5 <u>Privacy Impact Analysis</u>: Related to Characterization of the Information

<u>Privacy Risk:</u> There is a risk that the data in the ALM tool will be inaccurate if the data shared by the TIE from DHS authoritative sources is not accurate.

<u>Mitigation:</u> Data owners are required to perform data updates and validation of accuracy prior to providing data to the TIE and/or ALM. This update and accuracy check effort is performed to validate the integrity of the data being consumed. Additionally, each authoritative source has processes for validating its own data. Whenever data is amended, removed, or otherwise altered in the source systems, the same data changes upon the next data load into ALM. Data loads typically occur on a daily basis.

<u>Privacy Risk:</u> If changes are made to data in the authoritative source systems, there may be up to a 24 hour delay in updating the attributes in ALM based on the schedule for loading data into the ALM system.

<u>Mitigation:</u> This risk is partially mitigated. The frequency of these updates to TIE and ALM are based on requirements that are mutually agreed upon by DHS management stakeholders, as well as how often the source systems are able to perform updates based upon their technical capabilities. Any attribute changes made in the source systems will be updated within ALM upon the next data load, but no later than 24 hours after the change is made in the authoritative system.

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.

As described in Section 2.1 above, ALM is used to manage the identities and access rights of DHS employees and contractors with the goal of securing critical infrastructure by ensuring that users only have access to approved applications, and of streamlining the collection and sharing of digital identity data. During operations, ALM uses the identity and account attributes it collects about users to perform the functions described in Table 2.

<center>Table 2: ALM Functions</center>

Use	Description	How User Information is Used
Access Request and Automated Provisioning	ALM offers end users an easy-to-use self-service web portal for requesting additional access when needed. The tool has automatic workflows in place for approving or rejecting such requests. Typical approvals	When users request access to an application, ALM will either use

Use	Description	How User Information is Used
	are conducted by the user's manager and the Information System Security Officer (ISSO) for the application. It then automatically grants access if it is approved by the designated parties, or notifies the user if the request is rejected.	the information about that user[19] that is already known to create the account, or, if the application being requested requires additional information,[20] an electronic form may be presented to the user to collect additional information.
Access Certification	ALM periodically initiates reviews of user access rights to make sure that users still need their current level of access for their job functions. Designated reviewers receive a notification that requires them to either approve or revoke a user's access rights to a specific application.	Account and entitlement information is presented to the designated authority (e.g., the user's manager) for decision-making. Information presented to the designated decision-making authority does not include any sensitive PII.
Edit Identity Attributes	For a specific subset of attributes, the user will be allowed to either set or update the values of the attribute. The ALM tool will route these updates to a manager for approval.	Identity attributes are displayed to the user and his/her manager for validation. Information presented to the designated decision-making authority does not include any sensitive PII.
Separation of Duties	ALM allows for the definition of security policies. These define the rules for specific access or 'toxic' combinations of access that should not be possessed by a single user (e.g., Accounts Payable and Accounts Receivable). ALM can detect and automatically remove SoD violations according to established workflows when data is aggregated. It can also prevent them from occurring by prohibiting the user from requesting conflicting access.	Account and entitlement information about the user on whose account a violation has been detected is presented to the designated authority for decision-making. Information presented to the designated decision-making authority does not include any sensitive PII.
Access Reconciliation	ALM uses built-in workflows to identify, reverse, or remove changes that are made to accounts (e.g., creation, modification,	This is a backend function and data is not displayed to users. ALM uses account attributes to identify the

---

[19] See list and definition of "identity attributes" in Section 2.1.
[20] See definition of "account attributes" in Section 2.1.

Use	Description	How User Information is Used
	deletion) without going through the proper access request and approval process.	account in the backend system.
Off-boarding	ALM automatically disables accounts and removes all access rights when a user leaves the Department, but retains a record of his/her identity.	ALM uses identity attributes to identify the user and account attributes to identify which accounts to remove.

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?

ALM manages identities and access across all DHS Components (when fully implemented across all). Users are able to see and request access to applications within their Component, as well as enterprise applications available to all Components. As previously noted, ALM will be available for a limited set of users at DHS HQ followed by a broader DHS HQ rollout in FY17. The Component-by-Component rollout of ALM is currently slated for FY18-21. As the base of users increases, this PIA will be updated accordingly.

When ALM rolls out to Components, visibility into cross-component identities and applications will be controlled and limited to individual identities based on business rules (also known as 'scoping'). In other words, what a user is able to do and see in the ALM tool will be controlled by his or her job function within his or her individual DHS component. For example, a Compliance Officer for the Federal Emergency Management Agency (FEMA) would only be able to see details about users ("Identities") within FEMA. While the role of "Compliance Officer" determines what this specific user can do within the ALM tool, the scope of "FEMA" determines which population of users and segments of information this user can act upon. Users are assigned roles within the ALM tool that offer them certain capabilities, which may include: Application Administrator, Auditor, Certification Administrator, Entitlement Role Administrator, Policy Administrator, System Administrator, Help Desk Personnel, and Access Manager, among others. These roles can also be customized within the ALM tool in order to meet the requirements of individual DHS components. Each of these roles allows users to perform specific functionality

within the ALM tool that aligns with their job responsibilities while limiting the scope of the users and applications that they can see and act upon.

The exception to this is the limited number of Super Administrators with access across all of ALM for all components. Access to these accounts will be controlled by DHS's enterprise privileged management solution which monitors and controls administrative accounts.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: User information stored in the ALM solution may be inappropriately accessed or disseminated.

Mitigation: The ALM tool must store data in order to function as a solution. Access to the tool's database is only permitted by a system account that is used by the ALM application. ALM Administrators will require the use of a DHS enterprise privileged management solution to be able to access their privileged accounts in order to access the ALM database. Additionally, administrator privileges will only be granted to those users who have successfully completed the annual ALM recertification process.

The ALM user interface does allow users to access a view of their own information within the ALM tool. By default, a user can view his or her own identity and access rights, request additional access, or address items assigned to him or her. Any further actions that a user is able to perform in the tool are securely controlled by ALM based on the user's job function. Different users are therefore exposed to different views in the ALM self-service tool, and can only view information necessary within the parameters of their jobs. For example:

- A regular user can only view his or her own attributes;
- A manager can only view the identities of all employees who report to him or her; and
- An administrator can view those identities that fall within his or her jurisdiction (controlled by limiting the scope of identities based on a given business rule).

Further controls are in place to ensure the level of access is current and in line with established policies. This includes SoD, access recertification, and access conciliation, described in Section 3.1 above. Before ALM grants and grants access to an application, policies are set between ALM and the application owner. Once these are put in place, all access requests that are received are checked against established policy violations, and blocked or removed if necessary.

Users and systems will not query the ALM tool for Sensitive PII (e.g., clearance) attributes. These attributes will also not be exposed via the ALM dashboard used to complete access-related tasks. Other PII (e.g., name, email) will be visible to the access decision-making authority via the ALM dashboard. The only time PII could be shared will be if the ALM tool needs to write data to a given application's database and that specific application requires PII to function. In this case, the ALM PIA and design documents will be updated, and governance documentation will be

created to identify this sharing of information (e.g., Operational Level Agreement, Service Level Agreement, and Interface Control Document).

Privacy Risk: ALM writes to multiple consuming systems, increasing the spread of person information.

Mitigation: Use of ALM consolidates, secures, and automates the flow of identity information. Each connection to ALM will be documented, reviewed, and approved by the systems and data owners for both systems prior to implementation. Additionally, if user information needs to be written to an application, this will occur solely if the application has an approved PIA to receive the data.

Privacy Risk: There is a risk that Super Administrators may use their access to view personal information about individuals without an appropriate need to know.

Mitigation: The risk of Super Administrator access is mitigated by a three-tiered approach:

1. **Privileged Account.** In order for a user to become a super administrator, the user must first receive approval from his/her government supervisor as well as DHS Security. DHS Headquarters Risk Management Division (RMD) requires the user to complete the following training, which is validated on an annual basis, in order to receive a privileged account:

    a. DHS Role-Based IT Security Awareness training
    b. DHS HQ IT Computer Security Awareness and Rules of Behavior Training
    c. Privacy at DHS - Protecting Personal Information
    d. DHS HQ Incident Response Training
    e. Protecting Sensitive But Unclassified (SBU) Information Training

    After receiving a privileged account, the ALM ISSO will approve super administrator access to ALM and review the list of super administrator on an annual basis. The combination of training, RMD review, and ISSO review and approval ensures that only authorized personnel receive this level of access.

2. **Privileged Access Management Solution**. Access to the ALM servers is managed by the DHS Privileged Access Managmeent solution (i.e., Xceedium), which requires PIV authentication. Administrators are directly logged onto the server by the Privileged Access Managemnet solution, which logs, audits, and can record the user's session.

3. **ALM Audit capabilities**. ALM performs extensive auditing of user actions to include login to the tool and actions performed. Each log entry captures the user information in addition the timestamp the action was taken. The data center Security

Operations Center (SOC) monitors all system logs and reports questionable activities to the ISSO. The ISSO also reviews Event Logs monthly on the servers for any questionable activities.

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.

ALM does not provide notice prior to the collection of information because it does not collect information directly from individuals (see Section 2.2). Users are provided notice and consent to general uses of their information at the original point of collection when they submit their information (including identity attributes listed in Section 2.1) to DHS upon hiring, and employee or contractor onboarding as well as through this PIA and associated SORNs. The authoritative source systems listed in Section 2.2 and Appendix A provide Privacy Act Statements at the time of collection and have published SORNs to further provide notice to users.

For a select number of use cases, ALM may use electronic forms to collect information from users directly (see Section 2.2 for a description of a possible scenario). In this case, notice would be given to the user at the point of collection by the ALM user interface. In addition, tailored training will be provided to various user groups. Part of this training will include the request process and the potential need for notice at the point of collection. For more details on this process, see Section 8.2.

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

Any right to decline to provide information is exercised when choosing to be employed or contracted with DHS. ALM provides critical security and compliance features to manage access across the Department. As a security tool, users are not permitted to opt-out or circumvent the processes put in place by ALM.

4.3 Privacy Impact Analysis: Related to Notice

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

Mitigation: As a security solution, the use of ALM to manage user access is critical. Users will be trained on the benefits of ALM and how their information is being secured through a tailored communications and training campaign. Ultimately, ALM receives all information from the TIE, only after TIE authoritative sources have been reviewed and approved by DHS Privacy Office and other Department stakeholders. Users are provided notice, and consent to general uses of their information, when they submit their biographic and biometric attributes to DHS upon hiring and employee on-boarding. The authoritative source systems (detailed in Appendix A) all provide Privacy Act statements at the time of collection and have published System of Records Notices to further provide notice.

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.

Information about a user within ALM includes his or her identity information, account information, and audit trails of actions performed. Identity and account information provides a snapshot view of the access a user currently has. This information is updated to reflect any changes to his or her identity attributes or his or her access across systems at any moment in time. When the user leaves the Department, the identity record will be maintained in an inactive state within the ALM database. This record is retained for 6 years after the user is terminated, in accordance with General Records Schedule 3.2: Information Systems Security Records, Item 031, Disposition Authority DAA-GRS-2013-0006-0004.[21] Sensitive PII (e.g., clearance level) retained in the ALM database will be encrypted.

A historical record of attributes and access is not maintained. However, audit trails of actions performed will be maintained in compliance with the DHS 4300A Sensitive Systems Handbook and include:

- Access request, approval, provisioning;

- Access certification; and

- Policy violations.

---

[21] General Records Schedule 3.2: Information Systems Security Records, available at
http://www.archives.gov/records-mgmt/grs/grs03-2.pdf

5.2   Privacy Impact Analysis: Related to Retention

Privacy Risk: Identity information will be retained in the ALM tool even after the employee leaves the Department.

Mitigation: This risk is partially mitigated. All sensitive PII retained in the ALM database will be encrypted. Additionally, access to the identity information is limited to those who are authorized to view it. User access will be removed from the system upon termination, therefore only a record of his or her identity and his or her attributes prior to departure will be retained as directed by applicable records management requirements (see Section 5). The information related to access requests and certifications is retained for audit purposes.

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.

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

ALM does not share data with external entities.

6.3   Does the project place limitations on re-dissemination?

ALM does not share data with external entities.

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

ALM does not share data with external entities.

6.5   Privacy Impact Analysis: Related to Information Sharing

There are no privacy risks related to external information sharing.

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?

Users can access their identity information and access rights to applications at any time by logging into the ALM tool. ALM dashboard access is controlled through SSO, which allows users to authenticate to their computer with their PIV card and seamlessly access the ALM dashboard. By default, once users are logged in to the ALM tool, they can view their own identity and access, request additional access, or address items assigned to them.

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

If there is a discrepancy in the identity data, users can update certain attributes in the ALM tool, at which point this information would be routed to their manager for approval. Otherwise, redress would be sought from the system owners of the underlying source system listed in Section 2.2. The user works with his or her manager or calls the help desk to update his or her information in the authoritative source system (e.g., updates to a person's last name would have to be made through appropriate DHS processes; this data would be updated in ALM upon updates to the authoritative sources listed in Section 2.2). For information regarding redress in the authoritative source systems that provide attributes to ALM, see the respective PIAs and SORNs for each authoritative source system.[22] Once user information is altered in any way in the source system, ALM is updated to reflect that change upon the next data load. This is typically done on a daily basis.

If the user's access is not sufficient or incorrect, users can remove access from their accounts or request additional access using the ALM access self-service portal.

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

The procedures for correcting data in the underlying authoritative source systems that provide data to ALM via the TIE are set forth in the underlying PIAs and SORNs for the respective

---

[22] DHS/ALL/PIA-038(a) – Integrated Security Management System (ISMS) (September 16, 2014); DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System (August 23, 2012); DHS/ALL/PIA-043 – DHS Hiring and On-Boarding Process (April 22, 2013); and DHS/ALL/PIA-012(b) – E-Mail Secure Gateway (February 25, 2013), available at www.dhs.gov/privacy.

systems (see Section 2.2 and Appendix A). Standard Operating Procedures (SOP) vary by Component and are maintained by the Component Human Resources organizations.

Additionally, upon roll-out of the ALM tool, tailored training will be provided to different audiences across the Department. The internal DHS Access SharePoint site will also contain instructions and Frequently Asked Questions regarding ALM (http://mgmt-ocio-sp.dhs.gov/icam/dhsaccess/). A communications campaign to inform users of the functionality and roll-out of ALM will be conducted upon initial release. Finally, a help desk script will be provided to guide DHS Help Desk Personnel for calls related to ALM, including redress.

7.4 **Privacy Impact Analysis: Related to Redress**

Privacy Risk: While the ALM tool allows users to modify certain attributes as well as request or remove access, not all user attributes will be made available for direct updates or corrections by the user.

Mitigation: If a user determines an inaccuracy in his or her identity attributes, the user can follow the standard DHS protocol for updating their attributes through his or her manager or COR. Updates to the majority of identity attributes are held in Office of the Chief Human Capital Officer (OCHCO) and OCSO systems. All authoritative source systems are Privacy Act-covered systems and provide access, correction, and redress that will filter through to the TIE and to ALM.

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?

In order to ensure that information in the ALM tool is used in accordance with the stated practices in this PIA, the following actions will be taken:

- The project will go through the DHS security authorization process to demonstrate compliance with security controls (as explained in the ALM system security plan), including limiting access to data;

- Access to the information within the tool will be regulated using automated controls described in Sections 3.3 and 3.4, including controlling what a user is able to do within the tool based on his or her job function and the tool's scoping functionality;

- Built-in functions and workflows of the tool will monitor the system for violations related to access rights (e.g., access reconciliation and enforcement of SoD). The ALM tool

automatically detects, assesses, and reduces key risks while decreasing auditing and operational costs by continuously monitoring for policy violations and security threats; and

- Robust auditing, reporting, and analytics functions built into the ALM tool will provide an audit trail sufficient to reconstruct security-relevant events.

    o By default, ALM generates audit records for events such as: identity creation, identity modification, account deletion, account disabled, entitlement added, entitlement removed, entitlement request started, manual provisioning activity, provisioning completion, provisioning failure, and access request rejection, among others. These can be adjusted based on project needs. Additional auditing capabilities that can be enabled include events such as policy changes, system events, delegation, account privilege changes, and policy violation exceptions.

    o On demand, ALM can generate analytics and reporting for integrated systems on user accounts, entitlements, roles, access certifications, and policy violations.

        ▪ Note: ALM's ability to provide the aforementioned data points is dependent on the scope of the data provided and activities agreed to by the owners of the integrated systems. Detailed information on the data attributes and activities for each integrated system will be available via individual requirements documents.

- On an annual basis, whether via formal audit or self-initiated review, the following ALM tool and program elements will be reviewed for compliance and appropriateness:

    o Request, approval, provisioning, and user right and scoping approach processes for elevated access to ALM

    o ALM administrative SOP documentation

On an annual basis, ALM will conduct a certification of all accounts and workgroups which hold elevated access to ALM. Certifications will include account permissions, workgroup permissions, and workgroup membership. Following certification, reports including all entitlements, decisions, and reviewers involved in the certifications will be generated and remediation of accounts indicated for removal will be carried out. The ALM tool's very function is to onboard new hires efficiently and to detect and remedy access-related security violations. The system is able to protect DHS from modification or unauthorized access, or the destruction of the audit trail of accesses to the objects it protects.

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

All DHS employees and contractors are required to take mandatory security and privacy training prior to accessing a federal system. This security and privacy training course includes an overview on privacy, PII and its appropriate uses.

Additionally, as part of the ALM roll-out, a tailored communications and training campaign will be provided to different audiences across the Department. Specific training will be provided for different types of ALM users (e.g., a manager who will need to perform access approvals as part of his or her job function). As ALM is an end user-facing tool, all users will be trained in what the tool is able to do, how to interface with the tool, how to review their own information within the tool, how their information is being used, and of what workflows the tool is capable. In addition, training will cover the access request process, which may result in forms being presented to the user requiring him or her to enter his or her information. The training will cover the reasons for the information collection, the intent for the collection, and the benefits of the collection.

Moreover, the internal DHS Access SharePoint site will host instructions and Frequently Asked Questions regarding ALM.

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

All DHS employees and contractors will have access to the ALM tool by virtue of being employed or contracted at DHS. Access to the tool will be controlled through SSO, which allows a user to authenticate to his or her computer with his or her PIV card and seamlessly access the ALM dashboard. By default, a user of the ALM tool can view their own identity and access rights, request additional access, or address items assigned to him or her. Additional capabilities within the ALM tool are determined either through a user's job function (e.g., a manager will be able to approve or reject access for his or her direct reports) or can be requested and approved through the process described in the access request use case in Section 3.1. Controls will be in place to ensure that users are only able to access the information that they are allowed to see within the tool. This includes determining access based on a user's job function and scope (i.e., the component in which he or she works).

Additionally, any access to applications granted to users by the ALM tool will follow the access request and access certification processes described in Section 3.1. This includes periodically reviewing user access rights to ensure that access continues to align with job responsibilities.

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 Information Sharing Agreements or MOUs in place, because ALM will not share information outside of DHS.

Operational Level Agreements (OLA), Service Level Agreements (SLA), and Interface Control Documents (ICD) will be created in accordance with the DHS Information Technology Service Management (ITSM) Framework. These documents and agreements will be reviewed and approved by the ALM Project Manager, the ALM Program Manager (i.e., the Director of the Identity Services Branch), and the DHS Privacy Office.

Responsible Officials

Donna Roy
Executive Director
Information Sharing and Services Office
Office of the Chief Information Officer

Thomas McCarty
Director
Identity Services Branch
Office of the Chief Information Officer

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

_____

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

Appendix A – Authoritative Source Systems
Last updated May 7, 2021

This Appendix describes the DHS authoritative identity source systems used in TIE. If new authoritative identity source systems are added, this Appendix will be updated.

1. **The Chief Security Officer (CSO) Integrated Security Management System (ISMS)**

ISMS is the DHS Enterprise source of authority for personnel security information, including suitability, investigation status, and security clearance, for all DHS employees and contractors, for all DHS Components.

<u>Attributes provided to ALM</u>:

- Person Handle

- EDIPI

- First Name

- Middle Name

- Last Name

- City

- State

- Country

- Organization Code

- Organization Level 1

- Organization Level 2

- Employee Type

- Contract Number

- Clearance

- Status

- EOD Date

<u>ALM Refresh Rate</u>: Daily

PIA: DHS/ALL/PIA-038 Integrated Security Management System (ISMS).[23] ISMS is a web-based case management enterprise-wide application designed to support the lifecycle of the DHS personnel security, administrative security, and classified visit management programs.

SORN: DHS/ALL-023 Department of Homeland Security Personnel Security Management System of Records.[24]

2. **Human Capital Business Systems Enterprise Integration Environment (HCSB EIE)**:

The Human Capital Business Systems Enterprise Integration Environment (HCBS EIE) system is owned by the Department of Homeland Security (DHS) Headquarters (HQ) Office of the Chief Information Officer (OCIO) Information Sharing and Services Organization (IS2O) and the data is owned by the Office of the Chief Human Capital Officer (OCHCO) Strategic Workforce Planning and Analysis (SWPA). HCBS EIE is an Oracle data warehouse that contains data about DHS federal employees for all DHS Components, except for the U.S. Coast Guard military.

Attributes provided to ALM:

- Person Handle

- Organization Code

- Position Title

- Departure Date

- Executive Flag

- Manager

ALM Refresh Rate: Every two weeks

PIA: DHS/ALL/PIA-043 DHS Hiring and On-Boarding Process[25]

DHS/NPPD/PIA-009 Chemical Facility Anti-Terrorism Standards (CFATS)[26]

DHS/ALL/PIA-049 DHS Performance and Learning Management System (PALMS)[27]

DHS Enterprise Reporting

---

[23] DHS/ALL/PIA-038(a) Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.
[24] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).
[25] DHS/ALL PIA-043 DHS Hiring and On-Boarding Process, *available at* www.dhs.gov/privacy.
[26] DHS/ALL PIA-009 Chemical Facility Anti-Terrorism Standards (CFATS) *available at* www.dhs.gov/privacy.
[27] DHS/ALL PIA-049 DHS Performance and Learning Management System (PALMS) *available at* www.dhs.gov/privacy.

SORN: DHS/ALL-019, DHS/ALL-003, OPM/GOVT-1, and OPM/GOVT-2

3. The DHS Enterprise Directory

Sometimes also known as "AppAuth" or AD LDS (Active Directory Lightweight Directory Services), the DHS Enterprise Directory, operated by the Headquarters OCIO Enterprise Services Development Office (ESDO) contains Active Directory information (used to "log-on to the network") for all DHS employees and contractors, with few exceptions, such as the U.S. Secret Service and TSA Federal Air Marshals (FAMS) directories.

Attributes provided to ALM:

- EDIPI
- Email

ALM Refresh Rate: Daily

PIA: DHS/ALL/PIA-012(b) E-Mail Secure Gateway.[28]

SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[29]

4. Enterprise Reporting Application (ERA)

ERA provides data to ALM via the TIE. This data includes the Contracting Officer Representative (COR), start date, and end date for active task orders. ALM uses this information to associate contractors to a COR for the purposes of onboarding, off-boarding, and access to IT systems.

Attributes provided to ALM:

- Contracting Officer Representative Email
- Alternate Contracting Officer Representative Email
- Contracting Officer Email
- Contract Start Date
- Contract End Date
- Organization Level 1 that the contract is associated with (e.g., TSA, HQ, FEMA).

ALM Refresh Rate: Daily

---

[28] DHS/ALL/PIA-012(b) E-Mail Secure Gateway (February 25, 2013), *available at* www.dhs.gov/privacy.
[29] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).

<u>PIA</u>: DHS/ALL/PIA-081 DHS Management Cube.

<u>SORN</u>: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[30]

---

[30] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).