



Privacy Impact Assessment
for the

DHS Trusted Identity Exchange

DHS/ALL/PIA-050

April 2, 2015

Contact Point

Ashley Stevenson

Identity, Credential & Access Management (ICAM) PMO

Information Sharing Environment Office (ISEO)

Office of the Chief Information Officer

(202) 447-3348

Reviewing Official

Karen L. Neuman

Chief Privacy Officer

Department of Homeland Security

(202) 343-1717



Abstract

The DHS Trusted Identity Exchange (TIE) is a privacy-enhancing DHS Enterprise Service that enables and manages the digital flow of identity, credential, and access-management data for DHS employees and contractors. It does so by establishing connections to various internal authoritative data sources and provides a secure, digital interface to other internal DHS consuming applications. A consuming application is any DHS system that requires some form of identity, credential, and access-management data in order to grant logical or physical access to a DHS protected resource. DHS is publishing this Privacy Impact Assessment because TIE accesses and disseminates personally identifiable information (PII).

Overview

The DHS Headquarters (HQ) Office of the Chief Information Officer (OCIO) Information Sharing Environment Office (ISEO) Identity, Credential, & Access Management Program Management Office (ICAM PMO) is establishing the DHS Trusted Identity Exchange (TIE) in coordination with DHS Components.

TIE is being created to fill a major gap in DHS's current ability to effectively control and manage identity, credential, and access-management data (DHS ICAM data) about DHS employees and contractors.¹ Every internal DHS system, or "consuming" application, uses a unique collection of the user's digital identity and credential data to manage access to protected resources, such as federally managed facilities, information systems, and data. A consuming application is any DHS system that requires some form of identity, credential, and access-management data in order to grant logical or physical access to a DHS protected resource. Consuming applications may range from a physical building door reader to a computer connected to the DHS network, or to any application that resides on the DHS technical environment.

Digital identity data is often described as either "account" or "entitlement" information. Account information is used to *authenticate* (i.e., log-on) end users to verify they are who they say they are, and entitlement information is used to *authorize* the actions each user is allowed to perform on a given system. Individual components of a user's digital identity, called data attributes, reside in multiple systems across the enterprise, called "authoritative source" systems. Each data attribute resides in an authoritative source system, and may include personally identifiable information (PII). Updates or modifications to attributes are made in their respective authoritative source systems.

¹ 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.



The technology behind TIE is essentially a virtual directory. TIE establishes secure connections with authoritative systems, and then generates a secure, composite “view” of data attributes based on a combination of data fields from the source systems. TIE then provides these composite views to the consuming applications in a variety of system-to-system interfaces. Figure 1 depicts a graphical interpretation of how TIE will function.

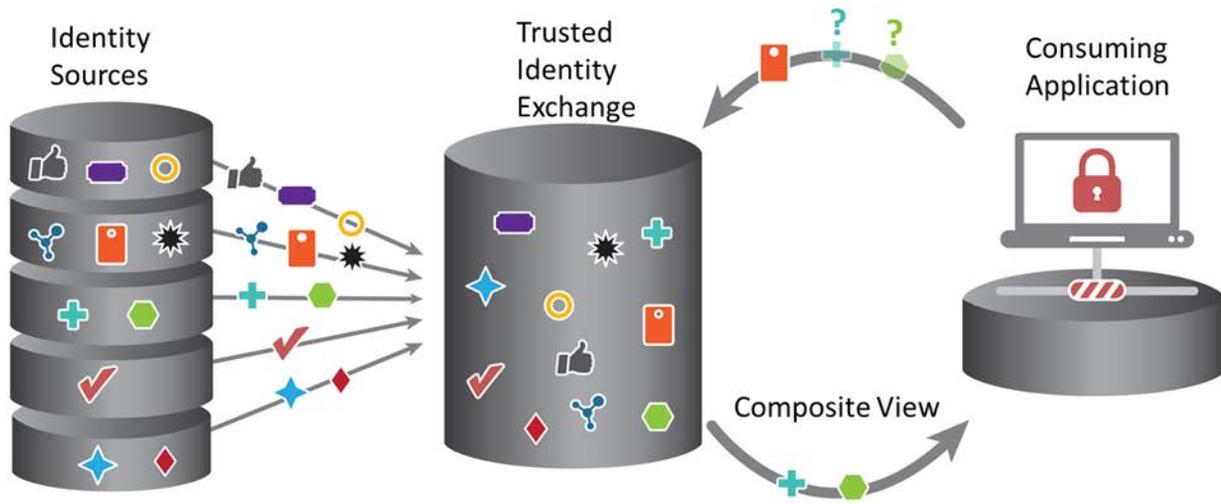


Figure 1: Graphical Overview of TIE Functionality

For performance reasons, TIE briefly holds or “caches” certain data attributes from the authoritative source systems and the consuming applications. This information only remains or “persists” in TIE until the authoritative source systems update the cache. Cache updates range from seconds to minutes or hours. TIE continuously overwrites or eliminates cached data based on updates from the authoritative source systems and the consuming applications.

Because TIE acts merely as a secure “broker,” the requirements for PII disposal or records archiving will persist from the underlying identity source system(s) or consuming application(s) that originally collect, manage, and store the data.

The high level TIE governance process will be driven by the joint OCIO/Office of the Chief Security Officer (CSO) ICAM Strategic Advisory Team (ISAT) and the joint OCIO/OCISO ICAM Executive Steering Committee (ESC).² The ISAT body is chartered to review and provide technical recommendations for decision votes at the ESC. The more granular level governance is handled by Memoranda of Understanding (MOU) and Interface Control Documents (ICD) between the authoritative source system owners, the DHS ICAM PMO, DHS Privacy Office, and the consuming applications.

² DHS Privacy Office is represented at both the ISAT and ESC.



Two practical examples below illustrate the nature of the process change with and without TIE.

Example One: Using TIE to provide a new employee with account access and to authorize what activities the employee can perform with his or her account:

Without TIE: A new federal employee is on-boarding to a DHS Component and requires basic access to the DHS network, email, facility control, training, and time & attendance systems. The present-day process causes multiple paper forms to be generated and sent via email or faxed to a number of individuals who must then hand-enter PII from paper forms, or lookup necessary information in other systems and copy and paste information into the systems for which the new employee needs access. Volumes of PII attributes are handled by multiple people through a series of relatively insecure business processes.

With TIE: Core identity information about DHS employees and contractors is available through TIE interface, which uses DHS digital policies to automatically provide the new employee's account access and authorization information in the network, email, facility control, training, and time & 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.

Example Two: Using TIE to support fine-grain authorization decisions.

Without TIE: Currently, authorizations to DHS systems and data are based on "point-in-time" information about users and are rarely re-evaluated or evaluated with enough frequency to ensure that only truly authorized individuals continue to be granted access.

With TIE: Attribute Based Access Control (ABAC) technologies query TIE interface (again via secure system-to-system, not human-to-system interface) and use the information, such as clearance status, training currency, organization, or location to make the final access decision. If a person's privacy training, for example, is required to be current in order to access certain data on a system, and the training certification expired yesterday, TIE will prevent the user from being granted access to the system today.³ This is because TIE will have a connection to the training system data, and will provide this necessary data to the consuming application in order to make the authorization decision.

³ Whether or not a user receives a reason for denied access is a function of the application, and out of scope for TIE. TIE simply supports the application decision-making process. Some applications may choose to tell the user why access is denied, while others, for security reasons, may not disclose this information.



The scope of TIE is limited to internal DHS ICAM data for authoritative sources, and to internal DHS consuming applications.⁴ This means TIE applies to the Sensitive but Unclassified (SBU) security domain, and is not scoped to directly serve National Security Systems on the classified domains (*i.e.*, “high side” applications). This also means that TIE does not directly share DHS ICAM data with non-DHS (external) systems. If DHS has a requirement to share one or more internal ICAM data attributes with an external partner, TIE may share approved attribute(s) with another DHS system (consuming application) that is ultimately responsible for sharing said attribute(s) outside of DHS.⁵

TIE is a key enabler to many important DHS initiatives, including the DHS Data Framework, fine-grain authorization (known as Attribute Based Access Control), Personal Identity Verification (PIV) Smart Card usage,⁶ and Single Sign-On (SSO). The following describe how TIE will impact each initiative.

DHS Data Framework

The DHS Data Framework is a scalable information technology platform with built-in advanced data security and access controls.⁷ TIE has been developed to meet the DHS Data Framework access control requirements. TIE will broker connectivity to the variety of authoritative identity data sources necessary to facilitate the authorization decisions required by the Framework.

Fine Grain Authorization

Today, most IT systems make and enforce access decisions based on static information that is provisioned at some point in time. A users’ level of access tends to remain the same in a given system, as most systems do not have automated procedures in place to “re-certify” that a given user or user community still has a valid need for a certain level of access. Fine-grain authorization (which sometimes materializes as ABAC) describes an IT system’s ability to make a final access determination based on near real-time information from authoritative identity sources. Because DHS has numerous authoritative identity sources, used by numerous consuming applications, TIE is necessary to provide a single interface (acting as a broker) for consuming applications to request the information required to make such a dynamic decision.

PIV Smart Cards

⁴ All TIE authoritative sources and consuming applications are listed in Appendix A and B.

⁵ This sharing is subject to DHS Privacy Office approval.

⁶ Personal Identity Verification (PIV) is a National Institute of Standards and Technology (NIST) specification, defined in the Federal Information Processing Standard (FIPS)-201-2. This standard was created under the direction of Homeland Security Presidential Directive (HSPD)-12.

⁷ The DHS Data Framework is DHS’s “big data” solution to build in privacy protections while enabling access to information across the DHS enterprise and with other U.S. Government partners. The DHS Data Framework will enable both search and analysis across currently stove-piped DHS databases in both classified and unclassified domains. For additional information about the DHS Data Framework, please see DHS/ALL/PIA-046 DHS Data Framework, available at www.dhs.gov/privacy.



Federal employees and contractors are issued PIV smart cards, which are secure credentials, and are required for use to access federally managed facilities and information systems. In order for these smart cards to be used as required by policy,⁸ TIE is required to broker connectivity between PIV authoritative sources and consuming applications in order to create an association between a person's PIV card and the related user account on any given system. The data attributes and PII required to provision⁹ and de-provision access accounts and entitlements is often moved via emails, spreadsheets, comma-separated value (CSV) files, and sometimes via fax. In order for a person to use his or her PIV card to log-on to the DHS network (Windows), data about the PIV card must be provisioned to Active Directory (AD).

Today, this is accomplished through a variety of manual processes, including several stop-gap solutions through which the provisioning takes place well after a person's AD account is created. In some instances, more information than is necessary may be transmitted between consumer and source systems to provision or de-provision access. These manual processes not only elevate the risk of exposing sensitive PII to unauthorized personnel, but also prohibit or hinder the efficient transfer of data required to securely grant access to users within the DHS infrastructure. TIE will serve as the identity information broker required to support automation of PIV and all other access entitlement provisioning and de-provisioning, thus eliminating costly, inefficient business processes. This facet of TIE also mitigates privacy risk by reducing the risk of exposure when PII is passed via less secure email or paper-based processes.

Single Sign-On (SSO)

SSO enhances a user's PIV log-on experience by enabling seamless, "one-click" access to applications, following use of the PIV card to log-on to the DHS network. SSO will reduce DHS's dependence on passwords for access to sensitive systems, while achieving PIV compliance. SSO enables an end-user experience that combines previously mentioned initiatives, such as PIV smart card usage, provisioning automation, and fine-grain authorization, and is a strategic initiative for DHS. In order to achieve the SSO user experience for all targeted applications, TIE must be in place to support PIV, provisioning, and fine-grain authorization use cases.

DHS Performance and Learning Management System (PALMS) Pilot

Presently, TIE is in a "production pilot" phase, serving the new Performance and Learning Management System (PALMS),¹⁰ an Office of the Chief Human Capital Officer (OCHCO) system,

⁸ See OMB M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractors," available at <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf>.

⁹ Provisioning and De-provisioning refers to the business processes and technologies employed to create accounts and entitlements in order to allow users to gain access to protected resources, such as federally managed facilities and information systems.

¹⁰ DHS/ALL-049 Performance and Learning Management System (PALMS) PIA (January 23, 2015), available at www.dhs.gov/privacy.



using identity information from the OCSO Integrated Security Management System (ISMS).¹¹ DHS OCIO is launching a production pilot to support provisioning and federated SSO for the new Performance and Learning Management System (PALMS).¹² For the production pilot, TIE will interface with the ISMS¹³ and the Active Directory Lightweight Directory Service (AD LDS) data. ISMS will act as the identity source system for DHS ICAM data, and AD LDS will provide the authoritative DHS email address for each identity. PALMS is the consuming application that will use or “consume” the ISMS and AD LDS data. Other authoritative identity source systems with which TIE will interface in the future are described in Appendix A. Future consuming applications will be brought on for TIE interface one at a time and will go through the governance process described above to determine which attributes will be provided depending on system requirements and use cases. Within this process, sensitive data like Social Security numbers (SSN) will only be provided to a consuming application following approval by governance stakeholders, including the DHS Privacy Office.

As additional authoritative sources and consuming applications are added to TIE, Appendices A and B of this PIA will be updated. If TIE program significantly changes following the pilot, DHS OCIO will complete a full PIA update.

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.¹⁴ 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. TIE is consistent with and promotes carrying out these responsibilities.

Relevant legislative and policy authorities for TIE include, but are not limited to the following:

- Federal Information Security Management Act of 2002, 44 U.S.C. § 3541 *et seq.*;
- Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (2004);

¹¹ DHS/ALL/PIA-038(a) - Integrated Security Management System (ISMS), available at www.dhs.gov/privacy.

¹² For additional information about DHS PALMS, please see DHS/ALL/PIA-049 Performance and Learning Management System (PALMS) available at www.dhs.gov/privacy.

¹³ DHS/ALL/PIA-038(a) - Integrated Security Management System (ISMS), available at www.dhs.gov/privacy.

¹⁴ *The Homeland Security Act of 2002*, Pub. L. 107-296, codified at 6 U.S.C. § 112 (2012).



- The Implementing the 9/11 Commission Recommendations Act of 2007, Pub. L. 110-53 (2007);
- Executive Order 12977, Interagency Security Committee, October 19, 1995;
- 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;
- Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011;
- Office of Management and Budget (OMB) Memorandum: Streamlining Authentication and Identity Management within the Federal Government (July 3, 2003);
- OMB Memorandum M-06-16: Protection of Sensitive Agency Information (June 23, 2006);
- OMB Memorandum M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007); and
- OMB Memorandum M-11-11: Continued Implementation of Homeland Security Presidential Directive (HSPD) – 12, Policy for a Common Identification Standard for Federal Employees and Contractors (February 3, 2011).

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

TIE is a broker between authoritative identity sources and consuming applications. TIE does not retrieve information by unique identifier. Therefore, TIE is not a Privacy Act system of records, therefore it does not require a SORN. TIE does not generate any unique identifiers, nor does it retrieve information by any unique identifiers from the authoritative source systems.

Authoritative identity sources and consuming applications that are Privacy Act systems of records, and their respective SORNs, are described in Appendix A and B.

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

At present, for the production pilot, TIE is hosted by the CBP ICAM system (CBP-06704-GSS-06704), which has a current ATO that is valid through August 31, 2015.

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

No. TIE does not retain any records. TIE briefly holds or “caches” certain data from its sources (*i.e.*, identity source systems and consuming applications). This information only remains or



“persists” in TIE until the identity source systems and consuming applications update the cache. Cache updates range from seconds to minutes or hours. The frequency of these updates will be 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. TIE continuously overwrites or eliminates cached data based on updates from these underlying sources.

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 TIE because TIE does not collect information from members of 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.

As described above, TIE disseminates existing information between DHS systems within DHS. TIE does not collect or store any information. TIE receives information originally collected by other underlying sources and does not collect or generate any original information. TIE brokers DHS ICAM data from numerous identity source systems within DHS.

The DHS ICAM data brokered by TIE includes the following types of information:

- **Biographic and Biometric**: The biographic and biometric categories represent a person’s “core identity” and may include data attributes such as name, date of birth, place of birth, parents’ names, home address, previous addresses, phone numbers, SSNs. Biometric attributes may include fingerprints, digital photographs, facial recognition coordinates. Please see Appendix A for a list of all current attribute information used by TIE. As this list expands or is modified based upon the data needs and requirements within TIE, the PIA will be updated.
- **Credential**: The credential category contains digital attributes about the credentials issued to person or machine identities. Common examples of credentials and their associated



attributes include PIV smart cards, Public Key Infrastructure (PKI) certificates,¹⁵ and system accounts. Credentials contain different types of data, depending on the type, but most include the subject's name, and some sort of number that is unique to the given class of credentials (not an SSN). For example, DHS PIV smart cards have a unique 10-digit number that is associated with the identity to which the card was issued.

- **Organization**: The organization category contains digital attributes about the organization to which a person or device belongs, and any specific attributes that a given organization collects, creates, and manages about a person or device. For example, organization information about the organization to which a person belongs could include Agency or Component name, supervisor name, and division, branch or section information. Examples of organization attributes that an organization collects, creates, or manages about a person or device will vary. For example, the Office of the Chief Security Officer, while vetting a candidate's suitability for federal employment will collect and manage organization-specific attributes such as creditworthiness and criminal history, while a human resources organization may collect (or generate) and manage attributes such as payroll, bank account, duty station, and required training information.
- **Entitlement**: The entitlement category contains information that is directly related to what level of access is given once a user is authenticated to a target system. This information may be distributed, and live on target systems, or may sometimes be centralized in certain identity systems. Examples of entitlement information include Access Control Lists (ACL), group membership, roles, or other attributes that are generated for the explicit purpose of granting access to a DHS protected resource. It should also be noted that, depending on the consuming application authorization requirements, identity attributes from the other categories, such as organization, biographic, or credential could also be used in making a final access determination. For example, a system could have an authorization rule that states "only someone who is part of organization "X" may access this system." In this case, the consuming application may ask TIE for information about the person's organization as part of the entitlement decision process.

Each identity source system and consuming application collects, generates, or otherwise manages some combination of the preceding DHS ICAM data categories. By defining these categories of data into logical or similar groupings with similar attributes, the DHS ICAM PMO will manage DHS ICAM data between the identity sources and the consuming applications in a more streamlined and effective manner.

¹⁵ PKI, as defined by NIST SP 800-32, is a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.



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

TIE does not create new information. TIE will broker information between numerous DHS systems; however, there are several key “core identity” systems that represent the majority of the DHS internal authoritative identity source systems. These systems are listed below:

- 1) The Office of the Chief Security Officer (OCSO) 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.
- 2) The OCSO PIV Identity Management System (IDMS): The PIV IDMS is 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 personnel, who use Common Access Card (CAC) smart cards. The CAC smart card credential information resides in a Department of Defense (DoD) system.
- 3) The DHS Enterprise Directory: Sometimes also known as “AppAuth” or 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.
- 4) The DHS Enterprise Certificate Authority: DHS “CA4” is the Enterprise PKI Certificate Authority for all Person Entity PKI certificates issued to DHS employees and contractors for all DHS Components, except for the U.S. Coast Guard.

The four preceding systems embody the majority of the DHS core identity (biographic and biometric) and credential authoritative identity source systems. These systems will be the primary providers of authoritative identity source information for TIE consuming applications. The systems that provide the data within the organizational and entitlement categories will vary across DHS components, based upon how and where the information is stored. Active Directory is one example of an authoritative source that will contain both organization and entitlement data.

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.

TIE is only the broker of information between the identity source systems and the consuming applications. The responsibility for maintaining accurate information lies with the source system and the consuming application. TIE continuously overwrites or eliminates cached data based on updates from these underlying sources.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk to data integrity since consuming applications will now rely on TIE for their identity credential, as opposed to the source systems. This may create data inaccuracies if the source data passed to TIE is not regularly refreshed.

Mitigation: As new source and consuming applications are added to TIE, the Appendices to this PIA will be updated to reflect the refresh rates. To promote accuracy and reduce data integrity risks, all authoritative source systems and consuming applications must have a refresh rate of at least daily updates to TIE.

Privacy Risk: Without TIE, the Fair Information Practice Principle of Data Minimization is at greater risk due to the tendency to repeatedly and redundantly move large volumes of privacy sensitive data through manual and relatively insecure business processes, including passing of information between numerous organizations and humans, each time increasing the risk of unintended exposure or disclosure of data.

Mitigation: Implementation of TIE mitigates existing privacy risks in DHS by eliminating the inconsistent application of user access controls to Department systems. TIE enhances the principle of data minimization due to TIE's ability to release only the required attributes, just in time, on a transactional basis, using more secure system-to-system interactions to the specific consuming applicants. This also significantly reduces the number of instances in which humans interact with the data, which may inadvertently leave a trail of forgotten files on hard drives, servers, email archives, etc.

TIE significantly reduces, and often eliminates, the likelihood of PII residing in systems once it is no longer required. First, in the case of dynamic, fine-grain authorization scenarios, such as ABAC, access entitlement information for users remains with the authoritative source systems, and is brokered by TIE in near-real time when required. This means that access entitlement data no longer resides or persists in many information systems, leaving a smaller PII footprint. Second, this same benefit applies with respect to PII account information in IT systems. Since TIE facilitates the automation of account provisioning and de-provisioning, PII will be removed from systems when it is no longer required, leaving a much smaller PII digital footprint across the enterprise.



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.

TIE is used to disseminate account and entitlement information between authoritative source systems and consuming applications to automate role-based access control. As noted above, TIE disseminates four different types of information attributes between the authoritative source systems and the consuming applications. Biographic and biometric attributes are used to positively identify an individual user. Credential attributes are used to match biographic and biometric attributes to person or machine identities. A credential is often considered "something you have," such as a PIV card. For example, DHS PIV smart cards have a unique 10-digit number that is associated with the identity to which the card was issued.

Organization attributes are used to differentiate between the different organizations and sub-units within the Department. The organization category contains digital attributes about the organization to which a person or device belongs, and any specific attributes that a given organization collects, creates, and manages about a person or device. These attributes are used to ensure that only those employees with a valid need-to-know have access to sensitive Department information. For example, the Office of the Chief Security Officer, while vetting a candidate's suitability for federal employment will collect and manage organization-specific attributes such as creditworthiness and criminal history, while a human resources organization may collect (or generate) and manage attributes such as payroll, bank account, duty station, and required training information.

Lastly, entitlement attributes are used to further narrow authorization rules for consuming applications. The entitlement category contains information that is directly related to what level of access is given once a user is authenticated to a target system. These access requirements are customizable by each consuming application. The entitlement option allows data owners to create very granular access for specific individuals who meet specific criteria. Entitlement attributes are used to further tailor access once a person has been positively authenticated based on biographic and biometric attributes, has a credential, and has resides in an approved organization. Consuming applications may use entitlement attributes to restrict access further to read-only, edit, administrator roles, for example.

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?

Due to the enterprise nature of TIE, most of the core authoritative identity source systems, described in section 2.1 already provide digital identity information to all or most of the DHS Enterprise. TIE will now provide that same information when the consuming application requests data, or has data pushed or provisioned to it from an identity source system. This scenario will apply to all DHS Components as it relates to the core authoritative identity systems referenced in section 2.1, as all of these systems already provide information or digital assets to most or all of the Components.

Finally, TIE will only broker information between internal DHS identity source systems and internal DHS consuming applications, with one exception: when DHS uses an external service provider for consuming applications, such as a public cloud software-as-a-service (SaaS) provider, TIE may provide basic account information to the external application in order to enable DHS employees and contractors to authenticate to these external systems. PALMS is a real-world example of this. Still, in these cases, it is the responsibility of the consuming application owners (such as DHS Office of the Chief Human Capital Officer for PALMS), whether the application resides on DHS premises, or in the cloud, to cover use of this information in their privacy documentation. For example, PALMS has published a separate PIA.¹⁶

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that TIE will provide information to consuming applications that is inconsistent with their missions or authorities. For example, not all consuming applications will require access to SSN or clearance information.

Mitigation: Attributes used by the consuming applications will vary based on their specific mission requirements. DHS will propose a set of standard, or “baseline” attributes and “attribute categories” for which any consuming application may consume using TIE system-to-system interface. Since TIE is merely an attribute broker, it is the responsibility of each consuming application to ensure that any attributes consumed from TIE are covered in the consuming application’s privacy documentation and subsequently approved by the DHS Privacy Office. Any additional attributes beyond the established baseline attributes proposed for TIE will first require the consuming application, the identity source system, or both to gain privacy approval through the development of project or system-specific privacy documentation.

In addition, TIE will provide a secure system-to-system interface for all brokered transactions. All consuming systems must first register with TIE, and validate that their requested use of information is covered and approved in their project or system privacy documentation. Once

¹⁶ DHS/ALL/PIA-049 Performance and Learning Management System (PALMS) PIA, available at www.dhs.gov/privacy.



this step is completed, the consuming application will receive access to the limited “baseline” set of attributes as previously mentioned, which will not contain highly sensitive attributes, such as SSN. Any consuming application requesting access to attributes from identity source systems’ attributes beyond the baseline, will need to provide justification, and show that use of this additional information is covered in the specific project or system privacy documentation.

For identity source systems, TIE will establish MOUs with each source system, listing the specific attributes that will be brokered by TIE. All MOUs must be approved by the governance structure described above, which includes the DHS Privacy Office.

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.

TIE 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 passed through TIE since there is no user interface. DHS is providing notice about TIE through this PIA. As described above, TIE does not collect information directly from individuals, but instead relies upon information collected by existing DHS authoritative identity source systems. These authoritative identity source systems are covered by existing SORNs, and provide Privacy Act Statements at the point of information collection.

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

Individuals do not have the opportunity to consent to the use of their data in TIE.

4.3 Privacy Impact Analysis: Related to Consent

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

Mitigation: TIE enhances the existing logical access control process for DHS systems. 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.

While an individual cannot consent to the use of their information in TIE, there is minimal privacy risk to the principle of individual participation because: 1) TIE does not store any



information and cannot make any adverse determinations based on the information it disseminates; and 2) TIE is only engaged when a user attempts to access a DHS system, to which the user has already consented to adhere to the relevant system Rules of Behavior and abide by all Department policies concerning system access.

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.

TIE does not retain information. TIE will cache data from identity source systems and consuming applications. Cache updates range from seconds to minutes or hours. Cached data is overwritten or eliminated based on these updates.

5.2 Privacy Impact Analysis: Related to Retention

Provided TIE continues to overwrite the existing cached data in near real-time, there are no privacy risks to data retention.

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.

TIE does not share data with external entities.

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

TIE does not share data with external entities.

6.3 Does the project place limitations on re-dissemination?

TIE does not share data with external entities.



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

TIE does not share data with external entities.

6.5 Privacy Impact Analysis: Related to Information Sharing

There are no privacy risks 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?

TIE is only an information broker, therefore, redress would be sought from the system owners of the underlying source systems (noted in Appendix A and B) containing the inaccurate or erroneous information.

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

Procedures to allow the subject individual (a DHS employee or contractor) to correct inaccurate or erroneous information are the responsibility of the underlying source system owner.

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

Because the data in TIE is the same as the data in the underlying systems, notification to individuals of the procedures for correcting data in TIE is the same as that of the underlying systems. Those procedures are set forth in the underlying SORNs for the systems (see Appendix A and B).

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 TIE's use of PII.

Mitigation: This risk is mitigated because TIE has near real-time refresh from all authoritative source systems. Individuals who believe the records used by TIE are inaccurate should contact DHS following the procedures detailed in Appendix A. All authoritative source systems are



Privacy Act covered systems and provide access, correction, and redress which will filter through to the TIE.

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?

As discussed previously, TIE will on-board each consuming application separately, issuing unique system-to-system credentials to each consuming application, and providing specific access control lists to determine the exact set of brokered attributes to which each consuming application has access.

TIE provides only for system-to-system interfaces, wherein a consuming application initiates an interface call to TIE to pull certain data attributes for the purposes of provisioning DHS ICAM data to a consuming application, or for a consuming application to make real-time authorization decisions based on the information provided by TIE interface.

Each interface to each consuming application will be defined and controlled, so that no consuming application will be able to request or receive attributes to which it has not been explicitly entitled.

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 TIE 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.

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

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



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 TIE does not share information. However, if the need arises, ICAM PMO will enter into MOUs as appropriate, and include the necessary level of review through all stakeholders, including the DHS Privacy Office.

Responsible Officials

Donna Roy
Executive Director
Information Sharing Environment Office
Office of the Chief Information Officer

Thomas McCarty
Director
ICAM PMO
Office of the Chief Information Officer

Approval Signature

Original signed copy on file with DHS Privacy Office.

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security



Appendix A – Authoritative Source Systems

(last updated on June 25, 2015)

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.

Attributes provided to TIE:

- Position and/or employee type based on job series;
- Name;
- Citizenship;
- Gender;
- Date of birth;
- DHS organization;
- Clearance level;
- Investigation status, including type and date;
- Duty station (city, state, country);
- Employee or contractor designation;
- Status;
- Contractor company name (if contractor);
- Contract number (if applicable);
- Agency;
- Job series; and
- Unique identifiers such as Person Handle and Electronic Data Interchange Personal Identifier (EDIPI).



TIE Cache Refresh Rate: Daily

PIA: DHS/ALL/PIA-038 Integrated Security Management System (ISMS).¹⁷ 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.¹⁸

2. The CSO PIV Identity Management System (IDMS)

The PIV IDMS is the DHS Enterprise source of PIV credential information, including credential identification and biometrics for all DHS employees and contractors for all DHS Components, except for the U.S. Coast Guard personnel, who use Common Access Card (CAC) smart cards. The CAC smart card credential information resides in a Department of Defense (DoD) system.

Attributes provided to TIE:

- PIV card unique credential identifiers such as EDIPI, Card Holder Unique Identifier (CHUID), Federal Agency Smart Credential Number (FASC-N), and Microsoft Explicit User Principal Name (UPN);
- Credential status (such as card type and expiration data);
- Foreign National status; and
- Entity Status.

TIE Cache Refresh Rate: Daily

PIA: DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System.¹⁹ This PIA provides detail about DHS's role in the collection and management of personally identifiable information (PII) for the purpose of issuing credentials (ID badges) to meet the requirements of HSPD-12 and comply with the standards outlined in FIPS 201 and its accompanying special publications. HSPD-12 requires a standardized and secure process for personal identity verification through the use of advanced and interoperable technology. This resulted in a need to collect biographic and biometric information. This PIA covers the information collected, used, and maintained for these processes, specifically the: (i) background investigation; (ii) identity proofing

¹⁷ DHS/ALL/PIA-038(a) - Integrated Security Management System (ISMS), available at www.dhs.gov/privacy.

¹⁸ DHS/ALL-023 Department of Homeland Security Personnel Security Management (February 23, 2010) 75 FR 8088.

¹⁹ DHS/ALL/PIA-014(b) Personal Identity Verification (PIV) Management System PIA (August 23, 2012), available at www.dhs.gov/privacy



and registration; (iii) Identity Management System (IDMS), the database used for identity management and access control; and (iv) the PIV card.

SORN: DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System.²⁰

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 TIE:

- Active Directory data, such as email address and user logon ID;
- User group membership;
- User organization info, such as department and supervisor (when available); and
- User contact info, such as name, work and home phone, and mailing address.

TIE Cache Refresh Rate: On-demand

PIA: DHS/ALL/PIA-012(b) E-Mail Secure Gateway.²¹ E-Mail Secure Gateway (EMSG) is owned by DHS and operated by DHS Headquarters (HQ). This service was previously managed under the Department of Homeland Security Directory Services Electronic Mail System (DSES). EMSG provides a single search point for DHS employees to locate other DHS employees’ contact information electronically, accessible by a web-based directory on the DHS intranet, or with e-mail client software. EMSG unifies DHS e-mail addresses from all DHS components into a single directory and provides a single route for incoming and outgoing e-mail. Each DHS component maintains control of its internal e-mail system and updates between their mail system directory and the EMSG DHS-wide directory. The system is made up of two portions: Directory Services and the E-mail System.

SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).²²

²⁰ DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).

²¹ DHS/ALL/PIA-012(b) - E-Mail Secure Gateway (February 25, 2013), available at www.dhs.gov/privacy.

²² DHS/ALL-004 - General Information Technology Access Account Records System (GITAARS), 74 FR 49882 (September 29, 2009).



4. The DHS Enterprise Certificate Authority

DHS “CA4” is the Enterprise PKI Certificate Authority for all Person Entity PKI certificates issued to DHS employees and contractors for all DHS Components, except for the U.S. Coast Guard.

Attributes provided to TIE:

- Digital credential identifiers, such as certificate serial number; and
- Credential identity data, such as Distinguished Name (DN) and Surname (SN).

TIE Cache Refresh Rate: On-demand

PIA: DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System.²³ In addition to broadly covering DHS compliance with the HSPD-12 requirements for the purpose of issuing credentials (ID badges), this PIA also discusses the Identity Management System (IDMS) which stores digital signatures (including PKI certificates) for DHS employees and contractors.

SORN: DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System.²⁴

²³ DHS/ALL/PIA-014(b) Personal Identity Verification (PIV) Management System PIA (August 23, 2012), *available at* www.dhs.gov/privacy.

²⁴ DHS/ALL-026 - Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).



Appendix B – Consuming Applications

(last updated on June 25, 2015)

This Appendix describes the DHS consuming applications that rely on the identity authentication provided by TIE. As new consuming applications are added, this Appendix will be updated.

1. DHS Performance and Learning Management System (PALMS) (April 2, 2015)

The DHS Office of the Chief Human Capital Officer (OCHCO) procured the DHS Performance and Learning Management System (PALMS) to facilitate the performance management process and consolidate the existing DHS Component learning management environments that support workforce training. DHS conducted this PIA because, when fully implemented, PALMS will collect, maintain, use, and disseminate PII about all DHS employees and contractors.

Consuming Application Refresh Rate:²⁵

- Bi-weekly

PIA: DHS/ALL-049 Performance and Learning Management System (PALMS)²⁶

SORNs:

- OPM/GOVT-1 - General Personnel Records;²⁷
- OPM/GOVT-2 Employee Performance File System Records;²⁸
- DHS/ALL-003 Department of Homeland Security General Training Records;²⁹
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS);³⁰ and
- DHS/ALL-037 E-Authentication Records System of Records.³¹

²⁵ The consuming application refresh rate refers to the frequency with which the consuming application makes calls to TIE. Some consuming applications will be ad-hoc, while others will be at scheduled intervals, depending on the use case.

²⁶ DHS/ALL-049 Performance and Learning Management System (PALMS) PIA (January 23, 2015), available at www.dhs.gov/privacy.

²⁷ OPM/GOVT-1 - General Personnel Records December 11, 2012, 77 FR 73694.

²⁸ OPM/GOVT-2 Employee Performance File System Records June 19, 2006, 71 FR 35342, 35347.

²⁹ DHS/ALL-003 - Department of Homeland Security General Training Records November 25, 2008, 73 FR 71656.

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

³¹ DHS/ALL-037 E-Authentication Records System of Records August 11, 2014, 79 FR 46857.



2. DHS Data Framework (June 25, 2015)

The DHS Data Framework is a scalable information technology program with built-in capabilities to support advanced data architecture and governance processes. It is DHS's "big data" solution to build in privacy protections while enabling more controlled, effective, and efficient use of existing homeland security-related information in both classified and unclassified domains. Adhering to the Framework will ensure access to the most authoritative, timely, and accurate data available in DHS to support critical decision making and mission functions.

Consuming Application Refresh Rate:

- Runtime during initial authorization decision process. TBD whether Data Framework will cache attributes or query on each authorization event.

PIA: DHS/ALL/PIA-046(b) DHS Data Framework³²

SORNs:

- DHS/CBP-009 - Electronic System for Travel Authorization (ESTA);³³
- DHS/ICE-001 - Student and Exchange Visitor Information System;³⁴
- DHS/TSA-002 - Transportation Security Threat Assessment System;³⁵
- DHS/CBP-016 - Nonimmigrant Information System;³⁶ and
- DHS/CBP-005 - Advance Passenger Information System (APIS).³⁷

³² DHS/ALL/PIA-046(b) DHS Data Framework PIA (February 27, 2015), available at www.dhs.gov/privacy.

³³ DHS/CBP-009 Electronic System for Travel Authorization (ESTA) July 30, 2012, 77 FR 44642.

³⁴ DHS/ICE-001 Student and Exchange Visitor Information System January 5, 2010, 75 FR 412.

³⁵ DHS/TSA-002 Transportation Security Threat Assessment System May 19, 2010, 75 FR 28046.

³⁶ DHS/CBP-016 Nonimmigrant Information System March 13, 2015 80 FR 13398.

³⁷ DHS/CBP-005 Advance Passenger Information System (APIS) March 13, 2015 80 FR 13407.