Privacy Impact Assessment
for the

DHS Trusted Identity Exchange

DHS/ALL/PIA-050(a)

July 21, 2017

Contact Point
Tarundeep Singh (System Owner)

Amir Dastouri (Branch Chief)
Identity Services Branch
Information Sharing and Services Office (IS2O)
Office of the Chief Information Officer
202447-5884

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

Abstract

The Department of Homeland Security (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 updating and replacing the original Privacy Impact Assessment (PIA) because TIE's expanded usage across DHS has created additional requirements.

Overview

The Department of Homeland Security (DHS) Headquarters (HQ) Office of the Chief Information Officer (OCIO) Information Sharing and Services Office (IS2O) Identity Services Branch established the DHS Trusted Identity Exchange (TIE) in coordination with DHS Components.

TIE was created to fill a major gap in DHS's 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.

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

[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.

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.

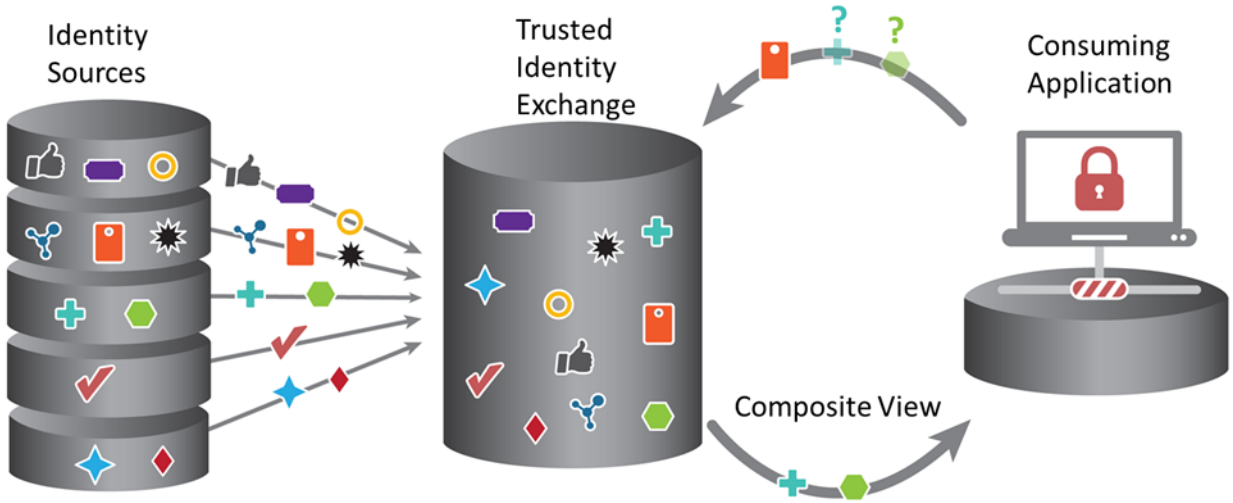

Figure 1: Graphical Overview of TIE Functionality

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/OCSO 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 Identity Services Branch, DHS Privacy Office, and the consuming applications.

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

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

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 previous process caused multiple paper forms to be generated and sent via email or faxed to a number of individuals who then had to 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 needed access. Volumes of PII attributes were 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: Previously, authorizations to DHS systems and data were based on "point-in-time" information about users and were rarely re-evaluated or evaluated with enough frequency to ensure that only truly authorized individuals continued 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 prevents the user from being granted access to the system today.[3] This is because TIE has a connection to the training system data, and provides this necessary data to the consuming application in order to make the authorization decision.

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

[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.
[4] All TIE authoritative sources and consuming applications are listed in Appendices A and B.

(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 impacts 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 brokers 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

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

[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.

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 provision[9] 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).

Previously, this was accomplished through a variety of manual processes, including several stop-gap solutions through which the provisioning took place well after a person's AD account was created. In some instances, more information than was necessary may have been transmitted between consumer and source systems to provision or de-provision access. These manual processes not only elevated 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 serves 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 reduces 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)

TIE serves the Performance and Learning Management System (PALMS),[10] an Office of the Chief Human Capital Officer (OCHCO) system, using identity information from the OCSO Integrated Security Management System (ISMS)[11] and OCIO Active Directory Lightweight Directory

[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) (January 23, 2015), *available at* www.dhs.gov/privacy.
[11] DHS/ALL/PIA-038(a) Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.

Service (AD LDS) to support provisioning and federated SSO for PALMS. ISMS acts as the identity source system for DHS ICAM data, and AD LDS provides 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.

As additional authoritative sources and consuming applications are added to TIE, Appendices A and B of this PIA will be updated.

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.[12] 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);
- 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;

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

- 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 Appendices A and B.

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

TIE is a minor application hosted by the DHS Access Lifecycle Management (ALM) system.[13] ALM will have an expected ATO date summer of 2017 and will be valid for a three-year period.

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. For more information regarding cache refresh rates by consumer and provider applications, please see Appendix A.

[13] For more information about the DHS Access Lifecycle Management (ALM) system, please *see* DHS/ALL/PIA-058 Access Lifecycle Management *available at* www.dhs.gov/privacy.

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 provides live views of information from source systems. In addition, TIE caches information on disk for performance purposes. This information is stored locally and updated per the cache refresh rates specified in Appendix A of this document. If the cache is removed, no data is retained on the TIE server. 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, Social Security numbers (SSN). 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, this 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,[14] 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

[14] 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.

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 Identity Services Branch manages DHS ICAM data between the identity sources and the consuming applications in a more streamlined and effective manner.

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) Human Capital Business Systems Enterprise Integration Environment (HCBS EIE): The EIE is the DHS enterprise human capital data warehouse that provides human resources attributes from the U.S. Department of Agriculture (USDA) National Finance Center (NFC) and the Web T&A system. EIE maintains data for all DHS employees, except for the U.S. Coast Guard.

4) 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 Transportation Security Administration (TSA) Federal Air Marshals (FAMS) directories.

5) 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. The TIE data is either live from the source system or cached locally for performance. The cache is continuously overwritten or based on updates from these underlying sources. Consistent with the refresh rates specified in Appendix A of this document, cache refreshing helps ensure the integrity of the data that is being consumed.

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. This information travels through manual and relatively insecure business processes, as well as 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 in Section 2.5, 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, etc.

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.[15]

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 has developed 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 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 provides 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 this step

[15] *See* DHS/ALL/PIA-049 Performance and Learning Management System (PALMS), *available at* www.dhs.gov/privacy.

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, as appropriate.

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 SORNs to further provide notice.

While an individual cannot consent to the use of his or her information in TIE, there is minimal privacy risk to the principle of individual participation because: 1) TIE does not permanently 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 as specified in Appendix A of this document.

5.2 Privacy Impact Analysis: Related to Retention

There are no privacy risks related to data retention. TIE either provides live views of data or caches locally for performance. The cached data is overwritten or eliminated. Local cache refresh rates for TIE are further specified in Appendix A of this document.

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 Appendices 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 Appendices 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 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?

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, the OCIO, IS2O Identity Services Branch will enter into MOUs as appropriate, and include the necessary level of review through all stakeholders, including the DHS Privacy Office.

Responsible Officials

Thomas McCarty
Director - Enterprise IT Services Division
Office of the Chief Information Officer

Pamela Freeman
Branch Chief - Identity Services Branch
Information Sharing and Services Office
Office of the Chief Information Officer

Approval Signature

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

_____

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

Appendix A – Authoritative Source Systems

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 employee types, for all DHS Components.

Attributes provided to TIE:

- Actionable Decision Date;
- Name;
- Date of Birth;
- Citizenship Country Code;
- Gender Code;
- Clearance Level;
- Clearance Status;
- SCI Status;
- Last Investigation Date;
- Last Investigation Type;
- Employee Status;
- Employee Type;
- Employee Type Group;
- Contractor Company Name;
- Contractor Contract Number;
- Contract End Date;
- Duty Location City;
- Duty Location Country;
- Duty Location State;
- Final Determination Decision;

- Final Entry on Duty (EOD) Decision Date;
- Is Position Primary;
- Job Series;
- Organization Code;
- Organization Level 1;
- Organization Level 2;
- Electronic Data Interchange Personal Identifier (EDIPI);
- Person Handle;
- Position Handle; and

TIE Cache Refresh Rate: Cache refreshes for ISMS occur daily.

PIA: DHS/ALL/PIA-038 Integrated Security Management System (ISMS).[16] 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.[17]

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:

- Name;
- ISMS ID;
- TP ID (database identifier not used for sharing);
- Investigation Status;
- Affiliation;
- Card Expiration Date;

[16] DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.
[17] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).

- Card Type;
- Card Auth Certificate;
- Card Auth Serial Number;
- Card Holder Unique Identifier (CHUID);
- Digital Signing Certificate;
- Digital Signing Serial Number;
- EDIPI;
- Encryption Certificate;
- Encryption Serial Number;
- Entity Status;
- Federal Agency Smart Card Number (FASCN);
- Organization;
- PIV Auth Certificate;
- PIV Auth Serial Number;
- PIV Card Status; and
- User Principal Name.

TIE Cache Refresh Rate: Cache refreshes for IDMS occur in near real-time.

PIA: DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System.[18] This PIA provides detail about DHS's role in the collection and management of 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 and registration; (iii) Identity Management System (IDMS), the database used for identity management and access control; and (iv) the PIV card.

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

SORN: DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System.[19]

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: Cache refreshes for AD LDS occur twice daily.

PIA: DHS/ALL/PIA-012(b) E-Mail Secure Gateway.[20] 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).[21]

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.

[19] DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).
[20] DHS/ALL/PIA-012(b) E-Mail Secure Gateway (February 25, 2013), *available at* www.dhs.gov/privacy.
[21] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 74 FR 49882 (September 29, 2009).

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: Cache refreshes for the DHS Enterprise Certificate Authority occur in near real-time.

PIA: DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System.[22] 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.[23]

5. Human Capital Business Systems Enterprise Integration Environment (HCBS 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 TIE:

- Person Handle;
- First Name;
- Middle Name;
- Last Name;
- Supervisory Code;
- Supervisor Person Handle;
- Supervisor Name;
- Series;
- EOD Date;

[22] DHS/ALL/PIA-014(b) Personal Identity Verification (PIV) Management System (August 23, 2012), *available at* www.dhs.gov/privacy.
[23] DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).

- Executive Flag;
- Location Code Description;
- Career Type;
- Political Appointee;
- Separation Date;
- Separation Description;
- Org Code;
- Org Level 1 Description;
- Org Level 2 Description;
- Org Level 3 Description;
- Org Level 4 Description;
- Org Level 5 Description;
- Org Level 6 Description;
- Org Level 7 Description;
- Org Level 8 Description;
- Time Keeper Person Handle;
- Web T&A Employee ID;
- Training Completed Date;
- Training Content ID;
- Training Content Title;
- Training Due Date;
- Training Equivalent Content;
- Training Extended Due Date;
- Training Period End;
- Training Period Frequency;
- Training Period;
- Email Address; and

- Component

TIE Cache Refresh Rate: Cache refreshes for HCBS EIE occur bi-weekly on average. Currently, NFC data is provided by the U.S. Department of Agriculture (USDA) as a report to OCHCO each pay period. As such, the data is only refreshed in EIE every two weeks.

PIA: DHS/ALL/PIA-043 DHS Hiring and On-Boarding Process[24], DHS/ALL/PIA-009 DHS Web Time and Attendance (Web T&A) System,[25] and DHS/ALL/PIA-049 Performance and Learning Management System (PALMS).[26]

SORN: DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records,[27] DHS/ALL-003 Department of Homeland Security General Training Records,[28] OPM/GOVT-1 General Personnel Records,[29] and OPM/GOVT-2 Employee Performance File System Records.[30]

6. Transportation Security Administration Pre-check Program (TSA Pre✓®) Opt-In Site

The Transportation Security Administration Pre-check Program Opt-In site provides DHS employees the ability to opt-in or opt-out of receiving the Pre-check benefit.

Attributes provided to TIE:

- EITIN (Known traveler number);
- Opt-In/Out;
- Date Last Updated; and
- Email Suffix.

TIE Cache Refresh Rate: Cache refreshes for TSA Pre-check occur daily.

PIA: DHS/TSA/PIA-041 Transportation Security Administration TSA Pre✓™ Application Program.[31]

SORN: DHS/TSA-021 TSA Pre✓™ Application Program System of Records.[32]

---

[24] DHS/ALL/PIA-043 DHS Hiring and On-Boarding Process, PIA (April 22, 2013), *available at* www.dhs.gov/privacy.
[25] DHS/ALL/PIA-009 DHS Web Time and Attendance (Web T&A) (May 1, 2008), *available at* www.dhs.gov/privacy.
[26] DHS-ALL-049 Performance and Learning Management System (PALMS) (January 23, 2015), *available at* www.dhs.gov/privacy.
[27] DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records, 80 FR 58283 (September 28, 2015).
[28] DHS/All-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).
[29] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[30] OPM/GOVT-2 Employee Performance File System Records, 71 FR 35342 (June 19, 2006).
[31] DHS/TSA/PIA-041 Transportation Security Administration (TSA) Pre✓™ Application Program (September 4, 2013), *available at* www.dhs.gov/privacy.
[32] DHS/TSA-021 TSA Pre✓™ Application Program System of Records, 78 FR 55274 (September 10, 2013).

7. Management Cube (MGMT Cube)

Management Cube consolidates information from departments across DHS to provide enhanced analytics capabilities. These capabilities are specifically designed to assess agency organizational performance and improve the quality and quantity of data that informs major decisions.

Attributes provided to TIE:

- City;
- Component Code;
- Country;
- County;
- Geo-coded Category;
- Master Location Identifier;
- Master Location Latitude;
- Master Location Longitude;
- Source Type;
- State;
- Street Address;
- Total Number of Components Located at Facility; and
- Zip Code.

TIE Cache Refresh Rate: Cache refreshes for MGMT Cube occur weekly. Currently, MGMT Cube data is provided by the Chief Readiness Support Officer (CRSO) on a quarterly basis and an automated email notification has been developed to notify the TIE team.

PIA: Forthcoming Management Cube PIA.

SORN: OPM/GOVT-1 General Personnel Records;[33] OPM/GOVT-2 Employee Performance File System Records;[34] OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers;[35] DHS/ALL-002 Department of Homeland Security Mailing and Other Lists System of Records;[36] DHS/ALL-019 Payroll, Personnel,

[33] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[34] OPM/GOVT-2 Employee Performance File System Records, 71 FR 35342 (June 19, 2006).
[35] OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers, 65 FR 24732 (April 27, 2000).
[36] DHS/ALL-002 DHS Mailing and Other Lists System, 73 FR 71659 (November 25, 2008).

and Time and Attendance Records System of Records;[37] DHS/ALL-023 Personnel Security Management System of Records;[38] and DHS/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records.[39]

8. Enterprise Reporting Application (ERA)

The Enterprise Reporting Application (ERA) is an information technology application that integrates the Department's contracting and procurement data. The application was developed as a business intelligence tool to collect and disseminate procurement-related information from disparate sources to enhance executive analysis decision making.

Attributes provided to TIE:

- Description of agency code for DHS procurement office;
- Agency code for DHS procurement office;
- Contract End Date;
- Contract Start Date;
- Contracting Officer Name;
- Contracting Officer Email Address;
- Contracting Officer Representative;
- Contracting Officer Representative Email Address;
- Unique Identifier for ERA data;
- Description for latest Federal Procurement Data System (FPDS) award;
- ID for award in FPDS;
- Modification Number;
- Contract Number; and
- Vendor DUNS number.

TIE Cache Refresh Rate: Cache refreshes for ERA occur daily.

PIA: Forthcoming Workforce Analytics and Employee Records PIA.

[37] DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records, 80 FR 58283 (September 28, 2015).
[38] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).
[39] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).

- SORN: OPM/GOVT-1 General Personnel Records.[40]

[40] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).

Appendix B – Consuming Applications

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)

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:[41]

- Daily

PIA: DHS/ALL-049 Performance and Learning Management System (PALMS).[42]

SORNs:

- OPM/GOVT-1 General Personnel Records;[43]
- OPM/GOVT-2 Employee Performance File System Records;[44]
- DHS/ALL-003 Department of Homeland Security General Training Records;[45]
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS);[46] and
- DHS/ALL-037 E-Authentication Records System of Records.[47]

2. Transportation Security Administration Secure Flight

The Transportation Security Administration Pre-check **(**TSA Pre✓®) program is one of several intelligence-driven, risk-based initiatives helping TSA provide the most effective security in the most efficient way on domestic and international flights. The program allows selected low-risk

[41] 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.
[42] DHS/ALL-049 Performance and Learning Management System (PALMS) (January 23, 2015), *available at* www.dhs.gov/privacy.
[43] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[44] OPM/GOVT-2 Employee Performance File System Records, 71 FR 35342 (June 19, 2006).
[45] DHS/ALL-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008).
[46] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).
[47] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).

travelers to experience expedited, more efficient security screening at participating U.S. airport checkpoints. TSA Pre✓® eligibility to all DHS Federal employees. In order to provide this service, TSA Pre✓® requires sensitive PII - specifically, name, date of birth, gender, and EDIPI information - for those DHS employees who opt in to receive TSA Pre✓® eligibility.

Consuming Application Refresh Rate:

- Daily

PIA: DHS/TSA/PIA-041 Transportation Security Administration TSA Pre✓™ Application Program.[48]

SORN: DHS/TSA-021 TSA Pre✓™ Application Program System of Records.[49]

3. Identity Credential Access Management (ICAM)

ICAM is a privacy-enhancing Department of Homeland Security Enterprise Service that enables and manages the digital flow of identity, credential, and access management data for DHS users, which includes both DHS employees and contractors, on the classified local area network or "C-LAN," the Department's Top Secret/Sensitive Compartmented Information (TS/SCI) network. ICAM establishes connections to various internal and Intelligence Community (IC) authoritative identity data sources and provides a secure, digital interface to other internal DHS consuming applications (systems that requires some form of identity, credential, and access management data in order to grant logical or physical access to a protected resource).

Consuming Application Refresh Rate:

- Daily

PIA: N/A.

SORN: DHS/ALL-004 General Information Technology Access Account Records System of Records.[50]

4. Policy Information Point Exchange Resource (PIPER)

PIPER 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 and certain non-DHS users of Secret-level applications. PIPER does so by establishing connections to various internal and external authoritative data sources and providing a secure, digital interface to other consuming applications. A consuming application is a system that requires some form of

[48] DHS/TSA/PIA-041 Transportation Security Administration (TSA) Pre✓™ Application Program (September 4, 2013), *available at* www.dhs.gov/privacy.
[49] DHS/TSA-021 TSA Pre✓™ Application Program System of Records, 78 FR 55274 (September 10, 2013).
[50] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).

identity, credential, and access management data in order to grant logical or physical access to a DHS protected resource. DHS will use PIPER to provide identity attributes to DHS Homeland Secure Data Network (HSDN) consuming applications for their use in access control decisions. In addition, PIPER will support the inauguration of the Secret Fabric Attribute Federation by entering into an agreement to exchange identity attribute information with the National Geospatial Intelligence Agency (NGA). The agreement will enable DHS to query for and receive responses containing identity attributes of NGA users accessing DHS-sponsored systems, and for NGA to query and receive responses containing identity attributes of DHS Users accessing NGA systems.

Consuming Application Refresh Rate:

- Daily

PIA: Forthcoming PIPER PIA.

SORN:

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS);[51]
- DHS/ALL-023 Department of Homeland Security Personnel Security Management;[52] and
- DHS/ALL-037 E-Authentication Records System of Records.[53]

5. 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.

Consuming Application Refresh Rate:

- Biweekly from OCHCO EIE

PIA: DHS/ALL/PIA-038 Integrated Security Management System (ISMS).[54] 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.[55]

---

[51] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 74 FR 49882 (September 29, 2009).
[52] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).
[53] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).
[54] DHS/ALL/PIA-038(a) Integrated Security Management System (ISMS), *available at* www.dhs.gov/privacy.
[55] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).

6. E-mail Secure Gateway (EMSG)

E-mail Security Gateway (EMSG) is used across DHS to route mail for the dhs.gov namespace. It includes mail hygiene and security services. Forefront Identity Manager (FIM) is a product within the accreditation of EMSG and is being provided data from TIE to automate the creation of email distribution lists.

Consuming Application Refresh Rate:

- Daily

PIA: DHS/ALL/PIA-012(b) E-Mail Secure Gateway.[56]

SORN:

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS);[57] and
- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System.[58]

7. FEMA Authentication and Provisioning Services (APS)

Authentication and Provisioning Services (APS) consists of the hardware, software, and data, which comprises the APS major application. APS includes ISAAC/FAMS/NACS and is used for Role based authorization to FEMA resources. The APS accreditation boundary includes Microsoft Windows Servers configured for Active Directory that provide authentication services and user management and control for access to network resources within the FEMA Enterprise Network; Microsoft Windows Servers/ Enterprise Oracle Red Hat Linux (RHEL) servers configured for ISAAC that provide password management capabilities and Role Based access configuration; and, Enterprise Oracle Red Hat Linux (RHEL) servers that provide password management capabilities and Role Based access configuration.

Consuming Application Refresh Rate:

- Daily

PIA: DHS/FEMA/PIA-031 Authentication and Provisioning Services (APS).[59]

---

[56] DHS/ALL/PIA-012(b) E-Mail Secure Gateway (February 25, 2013), *available at* www.dhs.gov/privacy.
[57] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 74 FR 49882 (September 29, 2009).
[58] DHS/ALL-002 DHS Mailing and Other Lists System, 73 FR 71659 (November 25, 2008).
[59] DHS/FEMA/PIA-031 Authentication and Provisioning Services (APS) (August 6, 2013), *available at* www.dhs.gov/privacy.

SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[60]

9. FEMA Physical Access Control System (PACS)

FEMA PACS performs automated validation of Personal Identity Verification (PIV) credentials in order to grant physical access to FEMA's buildings and facilities.

Consuming Application Refresh Rate:

- Daily

PIA: DHS/ALL/PIA-039 Perimeter Access Control System (PACS).[61]

SORN:

- DHS/ALL-024 Perimeter Access Control and Visitor Management;[62] and
- DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by DHS.[63]

10. USCIS Identity, Credential and Access Management (ICAM)/MyAccess application process

The USCIS Identity, Credential, and Access Management (ICAM) system provides USCIS employees and contractors with access to USCIS immigration systems and physical access to USCIS buildings through the employee's PIV card. USCIS will be using the requested attributes in a workflow to provision new users' accounts within USCIS. USCIS users log into MyAccess in order to gain access to ICAM.

Consuming Application Refresh Rate:

- Only during user on-boarding process

PIA: DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System.[64]

SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[65]

---

[60] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 74 FR 49882 (September 29, 2009).
[61] DHS/ALL/PIA-039 Perimeter Access Control System (PACS) (June 9, 2011), *available at* www.dhs.gov/privacy.
[62] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).
[63] DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by DHS, 75 FR 5614 (February 3, 2010).
[64] DHS/ALL/PIA-014(b) Personal Identity Verification (PIV) Management System (August 23, 2012), *available at* www.dhs.gov/privacy.
[65] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 74 FR 49882 (September 29, 2009).

11. CBP Identity, Credential and Access Management (ICAM) program

CBP ICAM provides enterprise Identity Management for CBP and its partners who are in need of a CBP identity/account to access CBP applications. CBP ICAM requires DHS user attributes from an authoritative source to identify the requests and to make an informed provisioning decision.

Consuming Application Refresh Rate:

- Twice a day

PIA: DHS/ALL/PIA-058 Access Lifecycle Management.[66]

SORN:

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS);[67] and
- DHS/ALL-037 E-Authentication Records System of Records.[68]

12. Management Cube (MGMT Cube)

Management Cube (MGMT Cube) consolidates information from departments across DHS to provide enhanced analytics capabilities. These capabilities are specifically designed to assess agency organizational performance and improve the quality and quantity of data that informs major decisions.

Consuming Application Refresh Rate:

- Daily

PIA: Forthcoming Management Cube PIA.

SORN: OPM/GOVT-1 General Personnel Records;[69] OPM/GOVT-2 Employee Performance File System Records;[70] OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers;[71] DHS/ALL-002 Department of Homeland Security Mailing and Other Lists System of Records;[72] DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records;[73] DHS/ALL-023 Personnel Security Management System of Records;[74] and DHS/ALL-024

[66] DHS/ALL/PIA-058 Access Lifecycle Management (January 24, 2017), *available at* www.dhs.gov/privacy.
[67] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 74 FR 49882 (September 29, 2009).
[68] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).
[69] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[70] OPM/GOVT-2 Employee Performance File System Records, 71 FR 35342 (June 19, 2006).
[71] OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers, 65 FR 24732 (April 27, 2000).
[72] DHS/ALL-002 DHS Mailing and Other Lists System, 73 FR 71659 (November 25, 2008).
[73] DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records, 80 FR 58283 (September 28, 2015).
[74] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).

Facility and Perimeter Access Control and Visitor Management System of Records.[75]

13. Access Lifecycle Management (ALM

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. LAM stores user information, including: identity attributes (*e.g.*, name, location, phone number, email) and application attributes (e.g., accounts that a user logs into an application with (username), specific attributes about a person required by the application).

Consuming Application Refresh Rate:

- Daily

PIA: DHS/ALL/PIA-058 Access Lifecycle Management (ALM).[76]

SORN: DHS/ALL-037 E-Authentication Records System of Records.[77]

14. ICE Investigative Case Management (ICM)

The Investigative Case Management (ICM) system serves as the core law enforcement case management tool primarily used by ICE Homeland Security Investigations (HSI) special agents and personnel supporting the HSI mission. Additionally, ICE Enforcement and Removal Operations (ERO) personnel use ICM to manage immigration cases that are presented for criminal prosecution. The ICE Office of Professional Responsibility (OPR) has read-only access to ICM as well as audit capability to conduct internal administrative or criminal investigations related to misconduct and/or misuse of ICM.

Consuming Application Refresh Rate:

- Daily

PIA: DHS/ICE/PIA-045 ICE Investigative Case Management (ICM).[78]

SORN: DHS/ICE-009 External Investigations.[79]

15. DHS Insider Threat Program (ITP)

The DHS Insider Threat Program (ITP) was established as a department-wide effort to manage insider threat matters within DHS. The Insider Threat Program was mandated by Executive Order 13587, which requires all federal agencies that operate or access classified computer networks, to establish an insider threat detection and prevention program covering all users of classified computer

[75] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).
[76] DHS/ALL/PIA-058 Access Lifecycle Management (January 24, 2017), *available at* www.dhs.gov/privacy.
[77] DHS/ALL-037 E-Authentication Records System of Records, 79 FR 46857 (August 11, 2014).
[78] DHS/ICE/PIA-045 ICE Investigative Case Management (ICM) (June 16, 2016), *available at* www.dhs.gov/privacy.
[79] DHS/ICE-009 External Investigations, 75 FR 404 (January 5, 2010).

networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), to ensure the security of classified networks and the responsible sharing and safeguarding of classified information on those networks with appropriate protections for privacy and civil liberties.

Consuming Application Refresh Rate:

- Multiple times a day

PIA: DHS/ALL/PIA-052 DHS Insider Threat Program.[80]

SORN: DHS/ALL-038 Insider Threat Program System of Records.[81]

16. 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.

Consuming Application Refresh Rate:

- Near real-time

PIA: DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System.[82]

SORN: DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System.[83]

17. MOBIUS

MOBIUS is a centralized repository of Enterprise Architecture (EA) used by DHS. DHS asset information contained within the MOBIUS include technology products and standards, systems, investments, services, agreements, and data architecture elements. MOBIUS is a consolidated source of DHS enterprise information and enables search, discovery, and reuse of assets across the Department. The system collects point of contact information DHS personnel to create user accounts.

Consuming Application Refresh Rate:

- Multiple times a day

PIA: DHS/ALL/PIA-006 DHS General Contacts List.[84]

[80] DHS/ALL/PIA-052 DHS Insider Threat Program (July 13, 2015), *available at* www.dhs.gov/privacy.
[81] DHS/ALL-038 Insider Threat Program System of Records, 81 FR 9871 (February 26, 2016).
[82] DHS/ALL/PIA-014(b) Personal Identity Verification (PIV) Management System PIA (August 23, 2012), *available at* www.dhs.gov/privacy.
[83] DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009).
[84] DHS/ALL/PIA-006 DHS General Contacts List (June 15, 2007), *available at* www.dhs.gov/privacy.

SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[85]

18. TSA News

TSA News is an employee communications mobile application only available to TSA personnel. Employees may download or remove the TSA News mobile app as they choose. TSA News retrieves news stories and distributes nationally relevant, non-SSI, non-classified information in real-time.

Consuming Application Refresh Rate:

- As needed

PIA: N/A.

SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[86]

19. TSA Online Learning Center (OLC)

TSA OLC is a cloud-based Learning Management System designed to deliver up-to-date, mission-relevant training material to all TSA Employees. The system provides TSA employees self-paced online courses, which permit each employee to manage their professional and personal development. TSA OLC is also a communication tool for getting job critical skills, knowledge, and information to TSA's Transportation Security Officers.

Consuming Application Refresh Rate:

- Daily

PIA: N/A.

SORN: DHS/ALL-003 DHS General Training Records.[87]

20. USCIS enterprise Physical Access Control System (ePACS)

USCIS ePACS is a component-wide program that allows USCIS personnel to request physical access to USCIS buildings and rooms through a self-service access web application that can be accessed by anyone with a USCIS email address. USCIS ePACS provides USCIS with a standard and secure method for approved users to request access to USCIS facilities and points of entry, while providing designated administrators with the ability to view and manage their user's access requests.

Consuming Application Refresh Rate:

- As needed

PIA: N/A.

SORN:

- DHS/ALL-023 Department of Homeland Security Personnel Security Management;[88]

[85] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 74 FR 49882 (September 29, 2009).
[86] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 74 FR 49882 (September 29, 2009).
[87] DHS/ALL-003 DHS General Training Records, 73 FR 71656 (November 25, 2008).
[88] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).

- DHS/ALL-024 Perimeter Access Control and Visitor Management;[89]
- DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by DHS.[90]

21. DHS HQ St. Elizabeth's Enterprise Physical Access Control System (PACS)

DHS HQ St. Elizabeth's (St. E's) PACS performs automated validation of Personal Identity Verification (PIV) credentials in order to grant physical access to FEMA's buildings and facilities.

Consuming Application Refresh Rate:

- Daily

PIA: DHS/ALL/PIA-039 (a) Perimeter Access Control System (PACS).[91]

SORN:

- DHS/ALL-024 Perimeter Access Control and Visitor Management;[92] and
- DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by DHS.[93]

22. FEMA Alert and Accountability Notification System (AANS)/AtHoc

AtHoc enables FEMA to communicate securely with personnel through agency issued devices during emergency events (e.g. active shooter, shelter in place, mandatory evacuation). It collects information from FEMA employees for situational awareness and personnel accountability before, during and after an event.

Consuming Application Refresh Rate:

- Daily

PIA: DHS/FEMA/PIA-036 Emergency Notification System (ENS).[94]

SORN: DHS/ALL-014 Department of Homeland Security Personnel Contact Information.[95]

23. S&T BACIS Attribute Consumer

The Science & Technology Border and Coastal Information System (BACIS) is a major application under the Coastal Surveillance System (CSS). CSS implements a framework for real-time information sharing that provides greater visibility across DHS component agencies and their partners of coastal and maritime activities, while enabling data source system owners to control the dissemination of data to protect the privacy of individuals. It acts as a bridge, redistributing data to vetted and authorized users in accordance with the sharing policy of the originating system owner.

---

[89] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).
[90] DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by DHS, 75 FR 5614 (February 3, 2010).
[91] DHS/ALL/PIA-039 Perimeter Access Control System (PACS) (June 9, 2011), *available at* www.dhs.gov/privacy.
[92] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).
[93] DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by DHS, 75 FR 5614 (February 3, 2010).
[94] DHS/FEMA/PIA 036 Emergency Notification System (ENS) (April 7, 2014), *available at* www.dhs.gov/privacy.
[95] DHS/ALL-014 Department of Homeland Security Personnel Contact Information, 83 FR 11780 (March 16, 2018).

Consuming Application Refresh Rate:

- Twice a day

PIA:

- DHS/ALL/PIA 038 Integrated Security Management System (ISMS);[96]
- DHS/ALL/PIA 012 Email Secure Gateway (EMSG);[97]
- DHS/S&T/PIA 033 Coastal Surveillance System (CSS).[98]

SORN:

- DHS/ALL-023 Department of Homeland Security Personnel Security Management;[99]
- DHS/ALL-004 General Information Technology Access Account Records System.[100]

24. Human Resources Business Engine (HRBE)

Customs and Border Protection (CBP) Human Resources Business Engine (HRBE). HRBE is a Human Resources System developed and maintained by CBP. It is used in multiple agencies across DHS and leverages AppAuth for authentication. For account provisioning CBP maintains multiple data feeds for individual agencies and would like to consolidate those to a single feed.

Consuming Application Refresh Rate:

- Daily

PIA:

- DHS/ALL/PIA-038 Integrated Security Management System (ISMS);[101]
- DHS/CBP/PIA-032 Human Resources Business Engine (HRBE); [102]

SORN:

- DHS/ALL-023 Department of Homeland Security Personnel Security Management;[103]
- DHS/ALL-024 DHS Facility and Perimeter Access Control and Visitor Management;[104]
- OPM/GOVT-1 General Personnel Records;[105]

---

[96] DHS/ALL/PIA-038 Integrated Security Management System (ISMS) (June 26, 2017), *available at* www.dhs.gov/privacy.
[97] DHS/ALL/PIA-012 Email Secure Gateway (EMSG) (February 25, 2013), *available at* www.dhs.gov/privacy.
[98] DHS/S&T/PIA-033 Coastal Surveillance System (CSS) (October 10, 2018), *available at* www.dhs.gov/privacy.
[99] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).
[100] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).
[101] DHS/ALL/PIA-038(c) Integrated Security Management System (ISMS) (June 26, 2017), *available at* www.dhs.gov/privacy
[102] DHS/CBP/PIA-032 Human Resources Business Engine (HRBE) (July 25, 2016), *available at* www.dhs.gov/privacy.
[103] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).
[104] DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management, 75 FR 5609 (February 3, 2010).
[105] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).

- OPM/GOVT-2 Employee Performance File System Records;[106]
- OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers;[107]
- OPM/GOVT-5 Recruiting, Examining, and Placement Records;[108]
- OPM/GOVT-6 Personnel Research and Test Validation Records;[109]
- OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records;[110]
- OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees File on Position Classification Appeals, Job Grading Appeals, and Retained Grade or Pay Appeals, and Fair Labor Standard Act (FLSA) Claims and Complaints;[111]
- OPM/GOVT-10 Employee Medical File System Records;[112]
- DHS/ALL-018 Administrative Grievance Records;[113]
- EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records;[114]
- DOL/GOVT-1 Office of Worker's Compensation Programs, Federal Employees' Compensation Act File;[115]
- OGE/GOVT-1 Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program;[116]
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS);[117]
- DHS/ALL-016 Department of Homeland Security Correspondence Records;[118]

---

[106] OPM/GOVT-2 Employee Performance File System Records, 71 FR 35342, 35347 (June 19, 2006).
[107] OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers, 65 FR 24732 (April 27, 2000).
[108] OPM/GOVT-5 Recruiting, Examining, and Placement Records, 79 FR 16834 (March 26, 2014).
[109] OPM/GOVT-6 Personnel Research and Test Validation Records, 71 FR 35354 (June 19, 2006).
[110] OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records, 71 FR 35356 (June 19, 2006).
[111] OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees, 78 FR 60331 (October 1, 2013).
[112] OPM/GOVT-10 Employee Medical File System Records, 75 FR 35099 (June 21, 2010).
[113] DHS/ALL-018 Administrative Grievance Records, 84 FR 18070 (April 29, 2019).
[114] EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records, 67 FR 49338 (July 30, 2002).
[115] DOL/GOVT-1 Office of Worker's Compensation Programs, Federal Employees' Compensation Act File, 77 FR 1738 (January 11, 2012).
[116] OGE/GOVT-1 Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records 78 FR 73863 (December 9, 2013).
[117] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).
[118] DHS/ALL-016 Correspondence Records, 83 FR 48645 (September 26, 2018).

- DHS/ALL-021 Department of Homeland Security Contractors and Consultants;[119]
- DHS/ALL-022 Department of Homeland Security Drug Free Workplace;[120]
- DHS/All-003 Department of Homeland Security General Training Records;[121]
- DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System;[122]
- DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records.[123]

25. St. Elizabeth's (St. Es) VoIP system

The St. Elizabeth's Voice over Internet Protocol (VoIP) system provides unified voice communications (off-net call, voice mail, audio conference, call center, E911, IM, presence) to DHS St. Elizabeth's Campus personnel. The VoIP system provides unclassified voice communications, voice teleconferences, voice mail services, and associated telephony equipment with connectivity throughout other DHS systems and the service provider's legacy PSTN.

Consuming Application Refresh Rate:

- Daily

PIA: N/A

SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[124]

26. St. Elizabeth's (St. Es) Physical Security Network (PSN)

The St. Elizabeth's (St. Es) Physical Security Network (PSN) is a collection of hardware and software tools designed to enhance detection and maintain surveillance of the physical grounds, buildings, and other network resources at the Department's St. Es Campus. The system collects sensitive PII, such as Social Security numbers, in order to verify a visitor's background and ensure their suitability for access to the site.

Consuming Application Refresh Rate:

- Daily

PIA:

- DHS/ALL/PIA-039 Physical Access Control System (PACS);
- DHS/ALL/PIA-014(c) Personal Identity Verification/Identity Management System (PIV/IDMS);
- DHS/ALL/PIA-042 Closed Circuit Television (CCTV).

[119] DHS/ALL-021 Department of Homeland Security Contractors and Consultants, 73 FR 63179 (October 23, 2008).
[120] DHS/ALL-022 Department of Homeland Security Drug Free Workplace, 73 FR 64974 (October 31, 2008).
[121] DHS/All-003 Department of Homeland Security General Training Records, 73 FR 71656 (November 25, 2008)
[122] DHS/ALL-002 Department of Homeland Security (DHS) Mailing and Other Lists System, 73 FR 71659, (November 25, 2008).
[123] DHS/ALL-019 Payroll, Personnel, and Time and Attendance Records System of Records, 80 FR 58283 (September 28, 2015).
[124] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012)

SORN:

- DHS/ALL-024 Department of Homeland Security Facility and Perimeter Access Control and Visitor Management;
- DHS/ALL-023 Personnel Security Management System of Records;
- DHS/ALL-025 Law Enforcement Authority in Support of Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security System of Records;
- DHS/ALL-026 Personal Identity Verification Management System of Records.

27. FLETC Ivanti Service Manager (ISM)

The FLETC Ivanti Service Manager (ISM), FLETC's new Identity and Access Management solution, enables FLETC to identify and verify employee on boarding and off boarding characteristics.

Consuming Application Refresh Rate:

- Daily

PIA: N/A

SORN:

- DHS/ALL-023 Personnel Security Management System of Records;[125]
- DHS/ALL-026 Personal Identity Verification Management System of Records.[126]

28. Joint-Threat Information Management System (J-TIMS)

J-TIMS is an enterprise-wide security solution developed by the Office of the Chief Security Officer (OCSO) to track and manage security threats across the Department. OCSO previously tracked security events through separate lines of business under different Divisions. To efficiently manage security case-related information across these divisions, OCSO developed J-TIMS.

Consuming Application Refresh Rate:

- Daily

PIA: DHS/ALL/PIA-084 Joint-Threat Information Management System (J-TIMS)[127]

SORN: DHS/ALL-023 Personnel Security Management System of Records[128]

29. ICE Federal Financial Management System (FFMS)

FFMS is a web-based, workflow management and financial transaction system that provides core financial management functions. It is used to create and maintain a record of each allocation, commitment, obligation, travel advance and accounts receivable issued.

Consuming Application Refresh Rate:

---

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

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

[127] *See* DHS/ALL/PIA-084 Joint-Threat Information Management System (J-TIMS), *available at* www.dhs.gov/privacy

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

- Daily

PIA: DHS/ICE/PIA-026 Federal Financial Management System[129]

SORN: DHS/ALL-004 General Information Technology Access Account Records System (GITAARS[130]

30. Parking and Transit Subsidy Application Tool (PTSAT)

PTSAT is a paperless transit and parking benefit program that will allow employees to enter and store their data.

Consuming Application Refresh Rate:

- Daily

PIA: XXXX

SORN: OPM/GOVT-1 General Personnel Records[131]

31. Trusted Identity Exchange Management Sunflower Asset Management System (TIE MGMT SAMS)

The Sunflower Asset Management System (SAMS) is used for tracking personal property and real property of several DHS components. Trusted Identity Exchange (TIE) enables the attribute consumer HQ MGMT SAMS accurate creation, updates, and end dates of personnel records in the property system of record for the Department of Homeland Security (DHS).

Consuming Application Refresh Rate:

- Daily

PIA: DHS/ALL/PIA-053 DHS Financial Management Systems[132]

SORN: DHS/ALL-010 Asset Management Records System of Records[133]

32. Army Financial Disclosure Management (FDM)

The Financial Disclosure Management (FDM) helps filers prepare and electronically file financial disclosure reports. FDM is a web-based initiative developed that was designed to provide a mechanism for individuals to complete, sign, review, and file financial disclosure reports. TIE enables the attribute consumer Army FDM to register new user and create an account in the FDM.

Consuming Application Refresh Rate:

- Daily

PIA: DHS/ALL/PIA-020 Financial Disclosure Management (FDM)[134]

SORN: Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records[135]

---

[129] *See* DHS/ICE/PIA-026 Federal Financial Management System, *available at* www.dhs.gov/privacy
[130] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).
[131] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[132] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[133] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[134] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[135] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).

33. ICE Repository for Analytics in a Virtualized Environment (R.A.V.En)

The information passed from TIE to ICE R.A.V.En pertains to all DHS users from all components. TIE enables the attribute consumer ICE R.A.V.En to use the selected attributes in order to properly support functionality in its applications, verify access and role based on the job series, and will use these attributes to notify an agent when a suspect's records hit against a database. Consuming Application Refresh Rate:

- Daily

PIA:

- DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System
- DHS/ALL/PIA-038 Integrated Security Management System (ISMS)
- DHS/ICE/PIA-055 Repository for Analytics in a Virtualized Environment (RAVEn)
- DHS/ALL/PIA-075 Workforce Analytics and Employee Records

SORN:

- OPM/GOVT-1 General Personnel Records December 11, 2012 77 FR 73694 , as modified by 80 FR 74815 (November 30, 2015)
- DHS/ALL-023 Department of Homeland Security Personnel Security Management February 23, 2010, 75 FR 8088
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System June 25, 2009, 74 FR 30301

34. MGMT SharePoint as a Service (SPTaas)

The information passed from TIE to MGMT SPTaaS pertains to all DHS components including USCG. TIE enables the attribute consumer MGMT SPTaaS to get the user profile information to authenticate users and allow single-sign on (SSO) with AppAuth.

Application Refresh Rate:

- Daily

PIA:

- DHS/ALL/PIA-059 DHS Employee Collaboration Tools

SORN:

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

35. CBP OKTA

CBP OKTA provides enterprise Identity Management for CBP and all DHS Components who are in need of a CBP identity/account to access CBP applications. CBP OKTA requires DHS user attributes from the DHS TIE to identify the requests and to make an informed provisioning decision.

Consuming Application Refresh Rate:

- Twice a day

PIA:

- DHS/ALL/PIA-058 Access Lifecycle Management.

SORN:

- DHS/ALL-004 General Information Technology Access Records System (GITAARS)
- DHS/ALL-037 E-Authentication Records System of Records
- DHS/ALL-023 Department of Homeland Security Personnel Security Management
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System
- DHS/ALL-003 Department of Homeland Security General Training Records
- DHS/ALL-037 E-Authentication Records System of Records.

36. FLETC Physical Access Control System (PACS)

The information passed from TIE to FLETC PACS pertains to all DHS employees and contractors from all the components. TIE enables the attribute consumer FLETC PACS to build API which will allow them to connect to TIE and pull user identity data to make decisions based on the attributes provided by TIE. The decisions that the FLETC PACS system will make is to provide access and assign roles to users as well as figure out what the contracting company name if the user is a contractor.

Application Refresh Rate:

- Daily

PIA:

- DHS/ALL/PIA-038 Integrated Security Management System (ISMS)
- DHS/ALL/PIA-039 Physical Access Control System (PACS)
- DHS/ALL/PIA-050 TIE

SORN:

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792
- DHS/ALL-023 Department of Homeland Security Personnel Security Management, October 13, 2020, 85 FR 64511

37. MGMT Counterintelligence Information Management System (CI2MS)

The information passed from TIE to MGMT CI2MS pertains to employees and contractors from all DHS components. TIE enables the attribute consumer MGMT CI2MS to build API which will allow them to connect to automate entity creation when a new DHS employee is found to be involved in a new CI matter and not already in the CI2MS system.

Refresh Rate:

- Daily

PIA:

- DHS/ALL/PIA-012(b) E-Mail Secure Gateway
- DHS/ALL/PIA-014 Personal Identity Verification/Identity Management System
- DHS/ALL/PIA-043 DHS Hiring and On-Boarding Proces
- DHS/ALL/PIA-050 TIE

SORN:

- OPM/GOVT-1 General Personnel Records, November 30, 2015, 80 FR 74815

- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS)

DHS/ALL-026 Personal Identity Verification Management System of Records

38. CBP Okta

The TIE will get identity attributes from CBP Okta. The consumer that will be getting these attributes is the CBP ICAM system. The CBP ICAM system must requested TIE to pull these attributes from CBP OKTA.

Okta provides Access Management (IaM) to various CBP systems and devices. Okta improves IaM across various devices and systems while also increasing security. Okta is compatible with the legacy on-premises systems and Cloud providers, thus reducing infrastructure complexity. Features and capabilities of Okta include: provisioning, Single Sign-On (SSO), Active Directory (AD) and Lightweight Directory Access Authentication. (LDAP) integration, the centralized provisioning of users, multifactor authentication (MFA), identity management and connectivity. The MFA is compatible with CBP's existing Personal Identity Verification (PIV) card.

The information being collected from CBP OKTA pertains to employees and contractors for all users in CBP OKTA system from all DHS components.

.Refresh Rate:

- Daily

PIA:

- DHS/ALL/PIA-050 Trusted Identity Exchange

DHS/ALL/PIA-058 Access Lifecycle ManagementSORN:

- DHS/All-003 Department of Homeland Security General Training Records November 25, 2008, 73 FR 71656
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792
- DHS/ALL-023 Department of Homeland Security Personnel Security Management, October 13, 2020, 85 FR 64511
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, June 25, 2009, 74 FR 30301
- DHS/ALL-037 E-Authentication Records System of Records, August 11, 2014, 79 FR 46857

39. TSA Infrastructure Core Services (ICS)

The information passed from TIE to TSA ICS pertains to TSA empolyees and contractors only. TIE enables the attribute consumer TSA ICS to perform the production of Information Technology (IT) assets necessary for the TSA to fulfill their mission of protection, security and customer service. ICS has already evaluated format/data of attributes requested in TIE DEV/Test environment and are making separate request

to get the attributes via TIE for production use. In addition to this, ICS will only get data from TIE DEV/Test environment, not from production.

Refresh Rate:

- Daily

PIA:

- DHS/ALL/PIA-014 Personal Identity Verification/Identity Management System
- DHS/ALL/PIA-038 Integrated Security Management System (ISMS)
- DHS/ALL/PIA-043 Office of the Chief Human Capital Officer Talent Acquisition
- DHS/ALL/PIA-050 DHS Trusted Identity Exchange
- DHS/ALL/PIA-075 Workforce Analytics and Employee Records

SORN:

- OPM/GOVT-1 General Personnel Records, November 30, 2015, 80 FR 74815
- DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), November 27, 2012, 77 FR 70792
- DHS/ALL-023 Department of Homeland Security Personnel Security Management, October 13, 2020, 85 FR 64511
- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, June 25, 2009, 74 FR 30301