Privacy Impact Assessment

for the

DHS Trusted Identity Exchange

DHS Reference No. DHS/ALL/PIA-050(b)

September 17, 2020

Homeland Security

Abstract

The U.S. 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 consuming applications. A consuming application is any system that requires some form of identity, credential, and access-management data in order to grant logical or physical access. DHS is updating this Privacy Impact Assessment (PIA) to discuss TIE's expanded sharing to consuming applications outside of DHS.

Overview

The DHS Office of the Chief Information Officer (OCIO) Solution Development Directorate (SDD) Platform and Solutions Division established TIE 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 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 system that requires some form of identity, credential, and access-management data in order to grant logical or physical access to a DHS or, in the case of this PIA Update, an Other Government Agency (OGA) resource. Consuming applications may range from a physical building door reader to a system or application connected to the DHS or OGA network.

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).

The technology behind TIE is essentially a virtual directory. TIE establishes secure connections with authoritative systems, and then generates a secure, composite "view" of data attributes based on a combination of data fields from the source systems. TIE then provides these

[1] "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.

composite views to the consuming applications in a variety of system-to-system interfaces. Figure 1 depicts a graphical interpretation of how TIE functions.

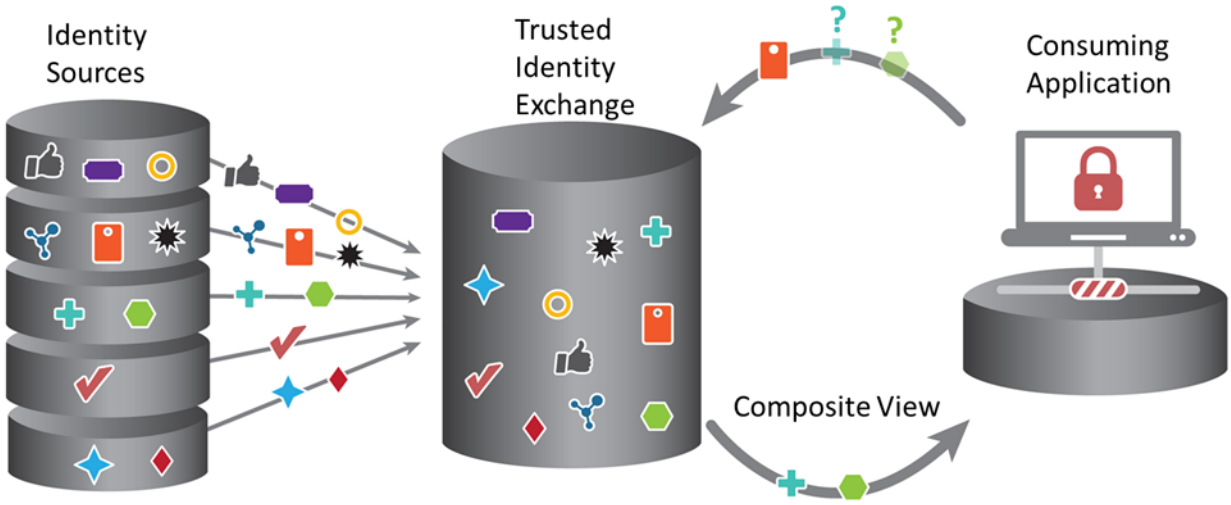

Figure 1: Graphical Overview of TIE Functionality

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.

Reason for the PIA Update

The purpose of this PIA Update is to account for connections and sharing with consuming applications external to DHS. The OCIO SDD Platform and Solutions Division has determined a need from its stakeholders to process attribute data for external applications (i.e., OGAs). TIE will continue to function in the same manner as described above and the previous PIA.[2]

Privacy Impact Analysis

Authorities and Other Requirements

The relevant legislative authorities and policy requirements for TIE have not changed with this update. 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

[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS TRUSTED IDENTITY EXCHANGE, DHS/ALL/PIA-050 (2017), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

appropriate databases of other departments and agencies.[3] TIE is a broker between authoritative identity sources and consuming applications.

The OGA consuming applications that are Privacy Act systems of records, and their respective system of records notice (SORN), are described in Appendix A. TIE is a minor application hosted by the DHS Access Lifecycle Management (ALM) system.[4] Since the last TIE PIA, ALM was re-accredited and has a valid Authority to Operate until July 2021.

Characterization of the Information

There are no changes to the types of information TIE process or sources of information as a result of this update. TIE still disseminates existing account or entitlement information from DHS authoritative source systems to consuming applications.

Uses of the Information

There are no changes to the uses of information as a result of this update. TIE is used to disseminate account and entitlement information between authoritative source systems and consuming applications, for example, to automate role-based access control. This data will now be shared with OGAs, but TIE and the information will still be used in the same manner.

Notice

It is difficult to provide notice to individuals that their information will be passed through TIE to an OGA consuming application. DHS is providing notice about TIE through this PIA Update. 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.

Additionally, TIE only passes information to a consuming application when there is a need for that consuming application to require the individual's attributes. For example, when the individual attempts to access the consuming application, TIE provides the attributes of the individual to ensure he or she should be provisioned access.

Privacy Risk: There is a risk individuals may not be aware that their information is being shared by TIE to an OGA.

Mitigation: This risk is partially mitigated. Individuals are provided notice, and consent to general uses of their information, when they submit their biographic attributes to DHS upon

[3] Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002) (current version in sections of 6 U.S.C.).
[4] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE ACCESS LIFECYCLE MANAGEMENT, DHS/ALL/PIA-058 (2017), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

hiring and employee on-boarding. The authoritative source systems (detailed in Appendix A of the previous PIA[5]) all provide Privacy Act Statements at the time of collection and have published SORNs to further provide notice.

While an individual cannot directly consent to the use of his or her information in TIE, there is minimal privacy risk 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 consuming application.

Data Retention by the Project

There are no changes to retention as a result of this update. TIE does not retain information; it only caches data from authoritative source systems to disseminate to consuming applications. Cache updates range from seconds to minutes or hours. Cached data is overwritten or eliminated based on the requirements of the authoritative source systems and consuming applications.

Information Sharing

TIE stakeholders have determined a need to share account and entitlement information to OGAs to provision access for DHS personnel on external systems. The information is technically shared in the same manner as data internal to DHS. The specific OGAs and uses cases are outlined in Appendix A below. The SORNs applicable to those uses cases are also listed in the appendix.

All new sharing connections go through an on-boarding process with oversight and approval from the authoritative source system owners, the Platform and Solutions Division, the DHS Privacy Office, and the consuming application owners. This includes the completion of a Privacy Threshold Analysis (PTA) and Memorandum of Understanding (MOU) and/or Interface Control Document (ICD), as appropriate. These discussions and documents provide a clear definition of what data may be shared by TIE and how that data may be used by the consuming application.

Privacy Risk: There is a risk information may be shared inappropriately outside of DHS to an OGA.

Mitigation: This risk is mitigated. The DHS Privacy Office has developed a close relationship with the Platform and Solutions Division to ensure a strict governance process for any new sharing connections. This includes the completion of a PTA for each initiative that requires input from the source system owners and consuming application owners. During this on-boarding process, the DHS Privacy Office includes the appropriate Component Privacy Office and conducts an analysis to ensure the use case meets all other privacy compliance requirements, adheres to DHS privacy policy, and only involves sharing of the necessary attributes.

[5] *See supra* note 2.

Redress

There are no changes to redress as a result of this update. TIE is only an information broker; therefore, redress should be sought from the system owners of the underlying source systems (noted in Appendix A of the previous PIA).

Auditing and Accountability

TIE on-boards each consuming application separately, issuing unique system-to-system credentials to each, and providing specific access control lists to determine the exact set of brokered attributes to which each consuming application has access. Each interface to a consuming application is defined and controlled, so that no consuming application is able to request or receive attributes to which it has not been explicitly entitled.

In addition, the OCIO SDD Platform and Solutions Division will enter into MOUs with all new OGAs, 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

Tarundeep Singh
TIE System Owner - Platform and Solutions Division
Solution Development Directorate
(202) 819-6275

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A – List of External Consuming Applications

1. **Army Financial Disclosure Management (FDM)**

FDM is a web-based initiative designed to provide a mechanism for individuals to complete, sign, review, and file financial disclosure reports. TIE enables FDM to register new users and create their accounts.

PIA: DHS/ALL/PIA-020 Financial Disclosure Management (FDM).[6]

SORN: OGE/GOVT-1 Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records,[7] and

DHS/ALL-004 General Information Technology Access Account Records System (GITAARS).[8]

2. **Transportation Security Administration (TSA) Online Learning Center (OLC)[9]**

TSA OLC is a web-based learning management system providing TSA's employees access to thousands of self-paced online courses and training materials, permitting employees to manage their professional development plan and automating the registration for internal and external training events. OLC influence reaches all areas of TSA with over 70,000 active users (including field employees, headquarters support employees, and contractors). OLC provides accurate up-to-date results of training and extracts, summarizes, and delivers data to a variety of governmental agencies regarding personnel performance.

PIA: N/A.

SORN: DHS/ALL-003 DHS General Training Records.[10]

3. **U.S. Coast Guard (USCG) Exchange[11]**

---

[6] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE FINANCIAL DISCLOSURE MANAGEMENT (FDM), DHS/ALL/PIA-020 (2008 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[7] *See* OGE/GOVT-1 Executive Branch Personnel Public Financial Disclosure Reports and Other Name-Retrieved Ethics Program Records, (78 Fed. Reg. 73863 (December 9, 2013), *available at* https://www.dhs.gov/system-records-notices-sorns.

[8] *See* DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 74 Fed. Reg. 49882 (September 29, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.

[9] Although this is a TSA consuming application, it requires an external connection.

[10] *See* DHS/ALL-003 DHS General Training Records, 73 Fed. Reg. 71656 (September 29, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.

[11] Although this is a USCG consuming application, it requires an external connection.

The USCG Exchange (https://shopcgx.com/) provides merchandise and services of necessity and convenience to retired and active USCG personnel, as well as other authorized patrons, such as other DHS personnel. USCG Exchange will use TIE to ensure that other DHS personnel who visit and make purchases at these exchanges or online are Active employees.

PIA: DHS/ALL/PIA-014 Personal Identity Verification (PIV) Management System.[12]

SORN: DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System.[13]

[12] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE PERSONAL IDENTITY VERIFICATION (PIV) MANAGEMENT SYSTEM, DHS/ALL/PIA-014 (2006 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[13] *See* DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 Fed. Reg. 30301 (June 25, 2009), *available at* https://www.dhs.gov/system-records-notices-sorns.