Privacy Impact Assessment Update
for the

Integrated Security Management System (ISMS)

DHS/ALL/PIA-038(b)

November 24, 2015

Contact Point
David Colangelo
Enterprise Security Services Division
Office of the Chief Security Officer
Management Directorate
(202) 447-5320

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Integrated Security Management System (ISMS) is a DHS-wide web-based case management application designed to support the lifecycle of the DHS personnel security, administrative security, and classified visit management programs. This Privacy Impact Assessment (PIA) is being updated to include the migration of Federal Protective Service users to ISMS, use of the Transportation Vetting System (TVS) to conduct continuous evaluation vetting during the background investigation process, and to reflect the use of ISMS as an authoritative identity source in the DHS Trusted Identity Exchange (TIE). DHS conducted this PIA because ISMS collects, maintains, uses, and disseminates personally identifiable information (PII) about federal employees and contractors.

Overview

In April 2008, the DHS Office of the Chief Security Officer (OCSO) implemented a web-based software solution, ISMS, to manage DHS personnel security and administrative security case records across the DHS security enterprise. ISMS facilitates the aggregate reporting that DHS provides to the Office of Management and Budget (OMB) and the Office of the Director of National Intelligence (ODNI). ISMS reduces the number of discrete interfaces that the Department must establish and maintain with external systems. ISMS also provides the ability to shift personnel security resources from one DHS component to another for surge support without incurring extensive retraining.

ISMS supports the lifecycle of DHS's personnel security, administrative security, and classified visit management records ("passing a clearance")[1] by managing data related to suitability determinations, background investigations, security clearance processing, security container and document tracking, personnel administration for security and classified contract support,[2] and incoming or outgoing classified visitor tracking. The records in this system reflect the tracking and status of activities related to the management and implementation of OCSO programs that support the protection of the Department's personnel, property, facilities, and information.[3]

[1] Classified visit management is an administrative process in which an individual's security clearance information is exchanged between agencies to document an individual's security clearance level.

[2] Note that some component personnel security divisions have the ability to manage contract or task order data in ISMS and then associate contractors to those contracts or task orders.

[3] This Privacy Impact Assessment (PIA) provides information on records maintained by OCSO within ISMS. Categories of individuals covered include: federal employees, applicants, excepted service federal employees, contractor employees, retired and former employees, and visitors who require: (a) unescorted access to DHS-owned facilities, DHS-controlled facilities, DHS-secured facilities, or commercial facilities operating on behalf of DHS; (b) access to DHS information technology systems and the systems' data; or (c) access to national security information including classified information. ISMS also covers state and local government personnel and private-sector

Reason for the PIA Update

DHS is updating this PIA to describe three changes to the ISMS system since the previous PIA publication:

1. *National Protection and Programs Directorate Federal Protective Service (NPPD FPS) Migration*

Since the last PIA update in September 2014,[4] NPPD FPS Protective Security Officer (PSO) personnel security data migrated to ISMS. FPS is an operational component of DHS NPPD. Its mission is to render federal properties safe and secure for federal employees, officials, and visitors. The migration is consistent with the Department's goal of integrated personnel security systems across all Components, increasing efficiency, and leveraging existing resources. As an enterprise-wide system, ISMS is now being used to manage personnel security information at DHS Headquarters, U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), U.S. Immigration and Customs Enforcement (ICE), U.S. Coast Guard (USCG), Transportation Security Administration (TSA), U.S. Secret Service (USSS), and NPPD FPS.

2. *Transportation Vetting System (TVS) Checks*

The OCSO Personnel Security Division (PSD) is responsible for ensuring that DHS employees are investigated and adjudicated for suitability to encumber a trusted position[5] and eligibility for access to classified national security information. In addition, Executive Order 13467 requires continuous evaluation of individuals determined eligible for access to classified information.[6] Continuous evaluation requires ongoing suitability checks to determine whether that individual continues to meet eligibility requirements.

ISMS currently transmits biographic details of the TSA workforce to TVS to conduct name-based matching against terrorist-related and watch list datasets.[7] To meet continuous evaluation requirements, OCSO PSD plans to use TVS to run recurrent vetting checks on the remaining portion of the DHS workforce holding national security positions. TVS checks will allow all component personnel security offices to review results of information prior to rendering a favorable determination as they would with any other investigative data.

individuals who serve on an advisory committee or board sponsored by DHS, or who require access to DHS facilities; and federal, state, local, and foreign law enforcement personnel who apply for or are granted authority to enforce federal laws on behalf of DHS.

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

[5] *See* Exec. Order No. 12968, 60 FR 40245 (Aug. 7, 1995).

[6] Exec. Order No. 13467, 73 FR 38103 (July 2, 2008).

[7] *See* DHS/ALL/PIA-027(c) Watchlist Service (WLS) Update, *available at* www.dhs.gov/privacy.

ISMS will use a similar process to the one currently in place for TVS screening of TSA employees. On a weekly basis, ISMS will create an XML file per population type (e.g., federal screeners, non-federal screeners, other TSA federal employees, other TSA contractors). These files will be encrypted and sent automatically via email to the TVS administrators for processing. Any hits will be reported directly back to a designated and trained point of contact in the appropriate component personnel security office who would receive the respective employee information. The new process will be piloted for the DHS HQ population to resolve any issues with the process prior to it being rolled out to DHS Components for use.

3. *DHS Trusted Identity Exchange (TIE) Connection*

As the DHS Enterprise source of authority for personnel security information, ISMS is an identity source system for TIE.[8] TIE manages information sharing between ISMS and a consuming application, which eliminates the need for ISMS to share copies of its data with individual systems.

Privacy Impact Analysis

In each of the below sections consider how the system has changed and what impact it has on the below fair information principles. In some cases there may be no changes and indicate as such.

Authorities and Other Requirements

No change from March 2011 PIA and September 2014 PIA update.

Characterization of the Information

Federal Protective Service (NPPD FPS) Migration

The NPPD FPS migration added a new PSO population of record subjects within ISMS; however, the information collected remains the same.

Transportation Vetting Service

Should information develop from the check of TVS, a new case will be created in the subject's personnel security file within ISMS for further investigation and evaluation. If the checks produce no results, no additional information will be stored in ISMS.

DHS Trusted Identity Exchange

ISMS data is being used by TIE to facilitate identity, credentialing, and access management requirements within DHS. No new ISMS data is created.

Uses of the Information

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

Federal Protective Service (NPPD FPS) Migration

ISMS use of NPPD FPS data is consistent with the previous PIA updates.

Transportation Vetting Service

ISMS shares the following PII with TVS for continuous evaluation screening on DHS employees holding national security positions:

- Full name;
- Personnel type;
- Gender;
- Date of birth;
- Place of birth;
- Social Security number;
- Citizenship; and
- Electronic Data Interchange Personal Identifier (EDIPI).

The suite of TVS checks currently run on TSA employees and planned for the rest of the DHS national security population includes weekly automated queries of Terrorist Screening Center watch lists. If the source list for one of the checks is updated with a new name, the list is automatically re-run in a process known as recurrent vetting. This is the case when a name is added or removed or when new information is available. In the event of a watch list hit, adjudicators work with the nominating agency and the screening center to determine whether the individual identified on the watch list is the same individual being screened.

DHS Trusted Identity Exchange

ISMS will serve as a data source for TIE and will provide the following data:

- Position and/or employee type based on job series;
- First, middle and last name;
- EDIPI;
- Citizenship;
- Gender;
- Date of birth;
- DHS Organization;
- Employee type (federal employee or contractor, and employee type group if applicable, e.g., TSA Transportation Security Officer);
- Clearance level;
- Investigation status (date and type of last investigation);
- Dates of suitability/fitness and onboarding determinations;
- Duty station;

- Contractor company name and contract number (for contract employees); and
- Employee status (active or inactive).

Privacy Risk: There is a risk that TVS checks will produce a false positive and misidentify an individual affiliated with DHS with an individual on a watch list.

Mitigation: Adjudicators research positive matches to validate that the information pertains to the same individual. The adjudicator coordinates with the screening center and the nominating agencies that originally placed the individual on the relevant list to resolve any potential identity discrepancies. As with information obtained from checks of other sources (for example, information identified from National Crime Information Center checks or subject interviews), all leads are fully investigated and validated against other information.

Notice

No change from March 2011 PIA and September 2014 PIA update.

Data Retention by the project

No change from March 2011 PIA and September 2014 PIA update.

Information Sharing

As outlined above, information sharing between ISMS and TVS will expand to cover the rest of the DHS national security population. ISMS data will be exported to TIE in accordance with the PIA.[9]

Redress

Individuals who suspect they have been placed on a watch list may request redress through the DHS Traveler Redress Inquiry Program.[10] Individuals who have been denied eligibility for access to classified information may submit a Freedom of Information Act (FOIA) request to obtain results of their background investigations. Some of these results may be exempt from disclosure under FOIA, such as sensitive security information, which includes "information and sources of information used by a passenger or property screening program or system, including an automated screening system," according to 49 CFR 1520.5 (b)(9)(ii).[11]

[9] *See* DHS/ALL/PIA-050 Trusted Identity Exchange, *available at* www.dhs.gov/privacy.
[10] *See* DHS/ALL/PIA-002(a) DHS Traveler Redress Inquiry Program, *available at* www.dhs.gov/privacy.
[11] *See* DHS/ALL/PIA-042 TSA Office of Intelligence and Analysis Technology Infrastructure Modernization

Privacy Risk: There is a risk that an individual with an unfavorable adjudication will not be able to correct inaccurate information due to the sensitivity of watch lists and other sources.

Mitigation: This risk is partially mitigated. Because TVS sources may not be disclosed, redress related to those sources is limited. This is consistent with the process for handling redress involving other sensitive sources in the personnel security process. For example, an interviewee providing adverse information on the subject may request that his or her identity not be disclosed. In such cases, as with other sensitive sources, the lead is investigated against other sources for corroborating information, thereby mitigating the risks posed by inaccurate information. Although specific watch list information may not be disclosed, all watch list hits are investigated against other sources for corroborating information. If information about the incident that resulted in the individual's placement on the watch list is available through other unclassified sources, then that information may be disclosed.

Auditing and Accountability

No change from March 2011 PIA and September 2014 PIA update.

Responsible Official

David Colangelo
Chief, Enterprise Security Services Division
Management Directorate, Office of the Chief Security Officer
Department of Homeland Security

Approval Signature

Original signed PIA on file with the DHS Privacy Office.

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security

Program, *available at* www.dhs.gov/privacy.