Privacy Impact Assessment Update
for the

Integrated Security Management System (ISMS)

DHS/ALL/PIA-038(a)

September 16, 2014

Contact Point
David Colangelo
Security Systems 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 web-based case management Department of Homeland Security (DHS) enterprise-wide application designed to support the lifecycle of the DHS personnel security, administrative security, and classified visit management programs.[1] This Privacy Impact Assessment (PIA) is being updated to include the migration of personnel security data and users from the United States Coast Guard (USCG), the Transportation Security Administration (TSA), and the United States Secret Service (USSS) to ISMS since the last approved PIA in March 2011.

Overview

In April 2008, the DHS Office of the Chief Security Officer (OCSO) implemented the Integrated Security Management System (ISMS), a web-based software solution to manage DHS personnel, administrative, and classified visit management security case records across the DHS security enterprise. Personnel security records maintained in ISMS include suitability and security clearance investigations that contain information related to background checks, investigations, and access determinations. ISMS also contains records associated with security container/document tracking, classified contract administration, and incoming and outgoing classified visitor tracking for administrative security and classified visit management.

Since the last approved PIA,[2] in March 2011, new DHS component personnel security data and users have migrated to ISMS. They include the United States Coast Guard (USCG), the Transportation Security Administration (TSA), and the United States Secret Service (USSS). The migration is consistent with the Department's goal of integrating personnel security systems across all components, increasing efficiency and leveraging resources. In addition, Immigration and Customs Enforcement has populated the Information Security (INFOSEC) tab, which contains facility information for all ICE facilities including locations; space; storage level; Facility Security Level (FSL); classified container information; and the local point of contact for each facility.

The migration of these DHS components to ISMS also created new capabilities, including:

Data export functionality (i.e., a stored procedure is executed to extract the data daily through which it is then encrypted and sent to the USCG through a secure File Transfer Protocol) allowing the USCG to export ISMS data to its Coast Guard Access and Coast

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

[2] DHS/ALL/PIA-038 Integrated Security Management System (ISMS), March 22, 2011, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhswide_isms.pdf.

Guard Business Intelligence system (CGBI) systems.[3] CGBI provides limited data sets to users requiring the information to determine and review classified access and vetting status (e.g., for access control offices to validate an individual's position and security clearance level, for security customer service to provide a prospective employee the status of his or her clearance investigation, or for recruiting offices confirm an individual's clearance level);

- Data export functionality (i.e., a daily ISMS job exports TSA data in a predefined format that is then zipped, encrypted, and then e-mailed to a specified e-mail address at TSA's Office of Intelligence and Analysis) allowing TSA to send personnel security data to the Transportation Vetting System (TVS) to conduct name-based matching against terrorist related datasets;
- Data export (i.e., a daily extract routine is executed using Informatica services) to the U.S. Customs and Border Protection (CBP) Data Warehouse enabling a stand-alone reporting tool in order to meet CBP's reporting needs (to include metrics and statistics on personnel duties surrounding the use of this data are captured in an Memorandum Of Understanding (MOU) between CBP and OCSO);
- Data export (i.e., a daily extract routine is executed using Informatica services) to the DHS Management Cube[4] providing and sustaining DHS cross-management performance measure reporting capability. However this file does not contain any personally identifiable information (PII) (i.e., no Social Security Numbers (SSN), names, or date of birth are used); and
- Data export (i.e., a weekly report that is manually exported and delivered to Office of Personnel Management (OPM)) to OPM allowing reporting of adjudicative decisions for non-OPM investigations. All data sent to OPM is encrypted and submitted through OPM's secure portal. An MOU between DHS and OPM spells out the requirements on how to transmit data via the secure portal.

[3] DHS/USCG/PIA-018 – Coast Guard Business Intelligence, April 17, 2012, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_cgbi.pdf.

[4] DHS Management Cube produces aggregate data and reports relating to the planning, programming, budgeting, and execution lifecycle, acquisition and investment decisions, general numbers of employees in an office, and other data that may be important for office decision making.

Reason for the PIA Update

This PIA is being updated to include the migration of USCG, TSA, and USSS personnel security data and users to ISMS since the last approved PIA in March 2011. In addition, ICE has populated the Information Security (INFOSEC) tab within ISMS.

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 practice principles. In some cases, there may be no changes as indicated.

Authorities and Other Requirements

In addition to the legal authorities and/or agreements mentioned in the March 2011 PIA, DHS maintains the results of the required background investigations in ISMS in accordance with the following Executive Orders and regulations:

1) Executive Order (E.O.) 12968, as amended, "Access to Classified Information," August 2, 1995;
2) Intelligence Community Directive Number 704, "Personnel Security Standards and Procedures Governing Eligibility For Access To Sensitive Compartmented Information And Other Controlled Access Program Information," October 1, 2008;
3) National Security Affairs Memorandum, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," December 29, 2005;
4) E.O. 10450, as amended, "Security Requirements for Government Employment," April 27, 1953;
5) DHS Delegation 12000, "Delegation for Security Operations within the Department of Homeland Security," June 5, 2012; and
6) Protected Critical Infrastructure (PCII): Critical Infrastructure Information Act of 2002, 6 U.S.C. § 131 *et. seq.*

In addition, a System Security Plan has been completed for ISMS, and an Authority to Operate was granted on May 20, 2014, by the DHS Information Systems Security Manager Certifying Official.

Characterization of the Information

No change from March 2011 PIA.

Uses of the Information

Since the March 2011 PIA, personnel security data and users from new components have migrated to ISMS, namely USCG, TSA, and USSS.

As an enterprise-wide system, ISMS is now used by all security offices within the Department. ISMS stores, manages, and partitions data by each component. A component may only access its own records. The information is shared between Department and component employees and contractors who require access to security eligibility and access-related information. Specific information about an individual will be shared with Department or component employees and its contractors in the performance of their duties who have a "need to know" in order to facilitate the personnel security vetting process. All employees must follow, and all Department contractors are contractually obligated to comply with, the Privacy Act in the handling, use, and dissemination of PII.

Personnel access ISMS data via an authenticated web interface. Access control is role-based and data is only accessible if a specific user has approved access to the data by his/her component's personnel security division chief.

The controls that are in place for internal sharing include the following:

- All ISMS users are required to complete, sign, and have their supervisor sign the ISMS User Account form, which also includes the ISMS Use Policy. Account forms are marked indicating that the end-user has requested cross-component roles.
- A limited number of component users are able to mark records as "limited access" records. Those records can only be viewed by users who have the limited access read-only role.[5]
- All records that are accessed by an end-user are logged. If there is concern that a record was accessed by an end-user for non-work related purposes, a report can be generated indicating all of the records that person has accessed.
- Components have the ability to create a "watch list" report. These reports flag records that have been accessed by end-users. The report lists the record that is flagged and the user who accessed the record. This report function was created at TSA's request. At this time, the reports are only sent twice a day to TSA's Personnel Security Office and TSA's Office of Intelligence and Analysis.
- The system tracks all changes that are made to a record. The system generates a remark in a remarks log that indicates the user who made the change, when the user made the change, what the previous value was, and how the value was changed.

[5] The "limited access" feature allows high profile records (i.e., the Secretary, Deputy Secretary) to be restricted to a limited set of users who have access to those records.

Privacy Risk: There is a risk a user will make an attempt to amend inaccurate data without following the proper policy and procedures.

Mitigation: Users are required to amend inaccurate data in ISMS by following the procedures outlined in the DHS Privacy Policy Guidance Memorandum 2011-01,[6] which indicates the system manager, in consultation with the component Privacy Officer or Freedom of Information Act Officer, as well as Counsel, shall make the determination as to whether to amend the record(s). Additionally, suspicious and/or unauthorized access is monitored and logged, thereby discouraging users from inappropriate access to the system.

Notice

DHS is updating this PIA to provide notice that ISMS is now used by all security offices within the Department. ISMS stores, manages, and partitions data by each component.

Data Retention by the project

No change from March 2011 PIA.

Information Sharing

Information is shared internally to facilitate security clearance reciprocity, access to controlled facilities, and federal reporting requirements. In addition to the systems mentioned in the March 2011 PIA, clearance information is shared with internal DHS systems to include: USCG Direct Access[7]; CGBI; CBP Data Warehouse; the TSA TVS; and the DHS Management Cube. Information is also shared externally with OPM. All federal agencies are required to report suitability and security clearance decisions to OPM. As mentioned in the overview section, DHS sends the adjudicative decisions made on investigations from third-party investigation providers (referred to as "Investigation Service Provider Investigations" (ISP-INV)) to OPM. As reported in the previous PIA (i.e., no change from March 2011 PIA), DHS also reports the adjudicative decisions for OPM investigations (also known as INV Form 79A, "Report of Agency Adjudicative Action on OPM Personnel Investigations").

If a DHS component chooses to share its data with another component, it can either assign the end-user the role or the Chief of Personnel Security for the component or it can send an e-mail to the ISMS Support team requesting that ISMS Support grant the roles for the end-

[6] Privacy Policy Guidance Memorandum 2011-01, "Privacy Act Amendment Requests," February 11, 2011, *available at*, http://www.dhs.gov/xlibrary/assets/privacy/privacy-policy-guidance-memorandum-2011-01.pdf

[7] Direct Access is a military web-based human resource system that collects and maintains all personnel attributes for Coast Guard members and contractors. For additional information, please see DHS/USCG-014 - Military Pay and Personnel System of Records, (October 28, 2011) 76 FR 66933, *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-10-28/html/2011-27881.htm.

user.

Background investigations, clearance verifications, and eligibility information, as well as relevant personal data for component records are shared with their respective systems:

1. USCG Direct Access, a third-party system maintained by USCG, requiring the investigative and clearance information of Military and Federal employees;
2. USCG CGBI, integrating USCG human resource data with personnel security data, allowing various non-personnel security users' read-only access to applicant status as well as clearance status;
3. TSA TVS, examining whether any of the TSA employees and contractor screeners and non-screeners are on Government watch lists;
4. CBP Data Warehouse, enabling CBP to maintain a stand-alone reporting tool to meet the demands of CBP's reporting requirements;
5. DHS Management Cube, providing and sustaining DHS's cross-management reporting capability; and
6. OPM ISP-INV, a new batch file process informing OPM of adjudicative decisions made on non-OPM investigations.

The following PII maintained in ISMS is shared with the USCG Direct Access system:

1. SSN;
2. Employee ID;
3. Security clearance level, type, status, and granted date;
4. Standard Form (SF)-312, "Classified Information Nondisclosure Agreement" briefed date;
5. Sensitive Compartmented Information (SCI) clearance certification dates including brief & debrief dates; and
6. Contact Security Clearance (SECCEN) flag.

The following PII maintained in ISMS is shared with the CGBI system:

1. SSN;
2. Employee ID;
3. Full name;
4. Date of birth;
5. Place of birth;

6. Citizenship;
7. Employee type;
8. Employee status;
9. Investigation type, case number, and status dates;
10. Security clearance level, type, status, and granted date;
11. SF-312 briefed date;
12. SCI eligibility;
13. Date paperwork received;
14. Date suitability adjudication;
15. Lautenberg (LAUT) issue flag;
16. Contact SECCEN flag; and
17. Date fingerprints adjudicated.

The following PII maintained in ISMS is shared with TSA TVS:

1. Full name;
2. Alias;
3. Personnel type;
4. Gender;
5. Date of birth;
6. Place of birth;
7. SSN;
8. Citizenship;
9. Passport information; and
10. Alien Registration Number.

The following PII maintained in ISMS is shared with DHS Management Cube:

1. Position ID number;
2. Electronic Data Interchange Person Identifier;
3. Organization;
4. Employee type;

5. Clearance level and date granted;
6. Last Investigation type and date;
7. Duty location;
8. Personal Identity Verification card status and last issue date;
9. Contractor company name and number;
10. Processing start date;
11. Initial Entry On Duty (EOD) decision and date; and
12. Final EOD decision and date.

The following PII maintained in ISMS is shared with OPM as part of the ISMS ISP-INV process:

1. SSN;
2. Full name;
3. Date of birth;
4. City of birth;
5. Country of birth;
6. Security Office Identifier;
7. Type of investigation;
8. Position sensitivity;
9. Applicant affiliation (Federal, Contractor);
10. Investigation initiation date;
11. Action (Completed, Discontinued)
12. SF used;
13. Issues;
14. OPM Investigation number assigned; and
15. Adjudication action and date.

ISMS provides a complete CBP data set to CBP for the CBP Data Warehouse to allow CBP to maintain reports independent of the ISMS Sequel Server Reporting Services (SSRS) tool. Data provided back to CBP was originated from CBP.

In addition to the privacy risks/mitigations described in the March 2011 PIA, the following privacy risk(s) and mitigation(s) pertaining to information sharing include:

Privacy Risk: There is a risk a user may send an individual's clearance information meant for one intended recipient to another, such as to the USSS rather than to TSA.

Mitigation: ISMS limits access and users are granted only those privileges that are necessary for their job requirements. The same roles that protect the system also determine which buttons and menu items are enabled for the user currently logged on. This ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes.

Redress

No change from March 2011 PIA.

Auditing and Accountability

No change from March 2011 PIA.

Responsible Official

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

Approval Signature

Original signed copy on file with DHS Privacy Office.

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security