Privacy Impact Assessment Update
for the

Personnel Security Activities Management System (PSAMS)/Integrated Security Management System (ISMS)

January 15, 2008

Contact Point
Kenneth Zawodny
Chief, Personnel Security Division
DHS Office of Security
officeofsecurity@dhs.gov

Reviewing Official
Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Office of Security (OS) uses the Integrated Security Management System (ISMS) to automate the tracking of Personnel Security related activities at DHS headquarters and component sites. ISMS is an update system to the Personnel Security Activities Management System (PSAMS). ISMS will help manage DHS personnel and security case records by adding to the existing functionality of PSAMS.

Introduction

The DHS Office of Security and each Component Security Office are responsible for vetting its' employees and contractors to ensure that they meet mandated suitability and security clearance standards. Currently, each DHS Component maintains its own security management system to store records related to this process. Additionally, each Component maintains a separate interface to various external systems maintained by the Office of Personnel Management (OPM) and the National Finance Center (NFC).

The DHS Office of Security has plans to implement a web-based software solution to manage DHS personnel and administrative security case records across the enterprise. The ISMS system will add to the existing functionality of the case management system in use by DHS Headquarters (i.e., PSAMS), and will replace five separate systems in use at Custom and Border Protection (CBP), Citizenship and Immigration Services (CIS), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), and Immigration and Customs Enforcement (ICE). ISMS supports the lifecycle of DHS's personnel and administrative security cases to include capturing the data related to all aspects of suitability determination, security clearance processing, security violation tracking, secure document tracking, and Contract Security Classification Specification (DD254) production.

Reason for the PIA Update

ISMS will replace the multiple security management systems currently in use across DHS HQ and Component organizations with a single commercial-off-the-shelf (COTS)-based enterprise-wide security management solution. The Office of Security has conducted market research to ensure that such a solution is commercially available. The solution provides a common repository for personnel security records across the Components facilitating the aggregate reporting that DHS must provide to the Office of Management and Budget (OMB) and the Office of the Director of National Intelligence (DNI). Furthermore, a consolidated system reduces the number of discrete interfaces that must be established and maintained with external systems. Finally, a consolidated solution provides the ability to shift personnel security resources from one Component to another for surge support without incurring extensive retraining.

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.

The System and the Information Collected and Stored within the System

Describe how this update affects the amount and type of personally identifiable information collected by the program or system, and how the update compliments the previously articulated purpose of the program

ISMS collects the same list of personally identifiable information (PII) as outlined in the PSAMS Privacy Impact Assessment (PIA). The primary difference in the amount and type of information collected and stored is that potentially disqualifying issues that may be identified during the adjudicative review process are documented and tracked within ISMS. In addition, the results from NCIC checks, credit checks, FBI name checks, results of any drug test (if administered), background investigations, and other personnel related data including but not limited to position grade, series, step, and pay plan may be stored. This information is stored to centralize case related documents and to shorten review and approval times associated with case processing. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, codified in Executive Order 13381 (6-27-05), mandates that agencies ensure the appropriate uniformity, centralization, efficiency, effectiveness, timeliness, and reciprocity of determining eligibility for access to classified national security information. Centralization and automation of related data as described in this update directly supports this mandate. Specific security roles have been defined within the application to control access to the data and the data is stored in encrypted fields or secured with file permissions if included as an attachment.

The ISMS system also introduces an information security (INFOSEC) module to support the tracking of classification authorities, guides, containers, documents, courier cards, DD254, and other INFOSEC related activities. The INFOSEC module integrates with the personnel security module (PERSEC) for identifying owners of INFOSEC elements (e.g., name, clearance level), but does not expose any other PII information to that module.

Depending on the type of investigation required, Executive Orders 10450, 10865, 12333, 12356, 12968 and 13311; Title 5 US Code (USC), sections 3301 and 9101; 42 USC sections 2165 and 2201; 50 USC sections 781 to 887; 5 Code of Federal Regulations (CFR) sections 5, 731, 732, and 736 provide the basis for collecting information regarding background investigations for suitability determination and National Security positions.

Protection of information associated with the system is described in DHS Management Directive (MD) 11042.1 Safeguarding Sensitive and Unclassified Information (FOUO), and DHS Policy for FOIA Compliance MD 0460.1

The only additional risk associated with this update is that additional information is being collected as outlined above. These risks are mitigated with the following security controls:

- Specific security roles have been defined and implemented within the application to control access to the additional information.

- Any additional information stored in large text fields will be stored in an encrypted form in the database
- When this additional information is stored as an attachment on the server, file access will be restricted by file permissions to prevent access by those without an appropriate requirement for access.
- Network access to the application is made via a Secure Sockets Layer (SSL) connection to the ISMS environment.

Uses of the System and the Information

Describe how the uses of the personally identifiable information have changed with this update and whether any privacy risks exist as associated with such changes.

The overall use(s) of personally identifiable information has not changed with the introduction of the ISMS update. However, in addition to the list of uses outlined in the PSAMS PIA, the ISMS system provides support to the following other security clearance related processes:

- Special Access
- Separation
- Periodic Reinvestigations
- Reinstate Security Clearance
- Security Clearance Downgrade
- Suspend/Withdraw
- Deny/Revoke Clearance
- Appeals

The only additional risk associated with this update is that additional information is being collected as described in the sections above. These risks are mitigated with the following security controls:

- Specific security roles have been defined and implemented within the application to control access to the additional information.
- Any additional information stored in large text fields will be stored in an encrypted form in the database
- When this additional information is stored as an attachment on the server, file access will be restricted by file permissions to prevent access by those without an appropriate requirement for access.
- Network access to the application is made via a Secure Sockets Layer (SSL) connection to the ISMS environment.

Retention

Describe whether retention schedules have changed or if the system now has an approved NARA schedule.

The implementation of ISMS does not require any change to existing security record or index retention schedules. The Personnel Security Division continues to follow NARA General Schedule 18, item 22a and 22c.

Internal Sharing and Disclosure

Describe how the internal sharing and disclosure have changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

In addition to the organizations outlined in the PSAMS PIA, the ISMS system will be deployed and used by Personnel Security Offices at CBP, CIS, FEMA, FLETC, and ICE. The data stored and managed by ISMS is partitioned by component so that only records belonging to that organization are viewable. Employees and contractors are required to go through ISMS as they were with PSAMS to obtain Security Clearances and Suitability screening processes. Privacy risks with information sharing have not changed and were mitigated previously implemented security controls.

External Sharing and Disclosure

Describe how the external sharing and disclosure have changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

External sharing and disclosure has not changed with the ISMS update. The ISMS update does not introduce any additional privacy risks in this area.

Notice

Describe whether additional notice is required to describe new collections, uses, sharing, or retention of the data and how that has or will be done.

The Office of Security Systems of Records Notice (SORN), DHS Office of Security 001 (71 FR 53700), and the published PSAMS Privacy Impact Assessment adequately covers how information is used. No additional notice is required.

Individual Access, Redress, and Correction

Describe how access, redress, and correction have changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

Individual access, redress, or correction has not changed with the ISMS update. The ISMS update does not introduce any additional privacy risks in this area.

Technical Access and Security

Describe how the technical access and security have changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

In addition to the organizations outlined in the PSAMS PIA, the ISMS system will be accessed by Personnel Security Offices at CBP, CIS, FEMA, FLETC, and ICE. Technical access and security will be expanded to these groups, but the overall approach and privacy risks associated with the system have not changed and were mitigated through previously implemented security controls.

Technology

Describe how the technology has changed with this update and whether any privacy risks have been identified and if they have, mitigation for such risks.

The technology areas listed below have been updated to support the implementation of ISMS. These changes do not introduce any additional privacy risk.

- Framework - ISMS is based on Security Manager, a COTS product that has been customized to meet specific DHS requirements not met in the core product. The system operates on the Microsoft platform and uses Microsoft SQL as the database technology. PSAMS also operates on the Microsoft platform using Oracle as the database technology. The change in back-end database technology does not introduce any additional privacy risks.

- Architecture - ISMS implements a web-based architecture, PSAMS implements a client-server architecture. The change in system architecture does not introduce any additional privacy risks.

- Operating Environment – The hardware supporting ISMS and PSAMS are physically located at a DHS Data Center.

- Security – ISMS and PSAMS have both undergone review and met the Certification and Accreditation (C&A) criteria required of a system hosting privacy data.

- Data Migration – A detailed data migration plan has been developed outlining the transition of data from PSAMS to ISMS. This plan details the mapping of specific data that will be transferred from the PSAMS system to the ISMS system so that existing status of existing security clearances and related processes will be maintained.

A report will be produced on the data migration process when it has been completed.

Responsible Official

Kenneth Zawodny
Chief, Personnel Security Division, Office of Security
Department of Homeland Security

Approval Signature Page

Original signed and on file with the DHS Privacy Office.

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security