# Privacy Impact Assessment Update
# for the
# Integrated Security Management System (ISMS)

**DHS/ALL/PIA-038(c)**

**June 26, 2017**


**Contact Point**

**Rosemarie Lawler**
**Enterprise Security Services Division**
**Office of the Chief Security Office**
**Management Directorate**
**(202) 447-5765**

**Reviewing Official**

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

## Abstract

The Integrated Security Management System (ISMS) is a Department of Homeland Security (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: 1) describe changes related to data retention and 2) reflect data collection of the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT)[1] encounters; polygraph events; and work email addresses. DHS is conducting this PIA because ISMS collects, maintains, uses, and disseminates personally identifiable information (PII).

## Overview

In April 2008, the Department of Homeland Security (DHS) Office of the Chief Security Officer (OCSO) implemented a web-based software solution, the Integrated Security Management System (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")[2] 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,[3] 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.[4]

---

[1] *See* DHS/NPPD/PIA-002 Automated Biometric Identification System (IDENT), *available at* https://www.dhs.gov/privacy.

[2] 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.

[3] 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.

[4] This PIA provides an update to the 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,

Due to the sysentive nature of the information stored in ISMS, the DHS Privacy Office will conduct a Privacy Compliance Review on the system.

## Reason for the PIA Update

DHS is updating this Privacy Impact Assessment (PIA) to describe several changes to ISMS since the previous PIA publications.[5]

*Data Retention*

ISMS records shall follow the retention guidelines outlined in National Archives and Records Administration (NARA) General Records Schedule (GRS) 5.6 Security Records (update to GRS 18).[6]

*Data Related to IDENT Encounters*

The ISMS record for an individual may contain the results of matches from biometric (*e.g.*, fingerprint) checks submitted to the Office of Biometric Identity Management (OBIM) Automated Biometric Identification System (IDENT). Information from IDENT is transferred to the DHS Identity Management System (IDMS)[7] and then to ISMS. ISMS tracks the encounter identifier, date, reason for the encounter, activity description, and watch list code, along with other information listed in the *Characterization of the Information* section below. While this IDENT data is new information that is being consumed by ISMS, there has been an existing connection between ISMS and IDMS because ISMS is the system of authority for IDMS.[8]

*Data Related to Polygraph Events*

The ISMS record for an individual may contain polygraph data on that individual when his or her job series or position requires the completion of a polygraph as part of the personnel security adjudication process. Component users manually enter polygraph data into ISMS. ISMS tracks the

---

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 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.

[5] For more information about ISMS, please *see* DHS/ALL/PIA-038 Integrated Security Management System (ISMS) and its associated updates, *available at* https://www.dhs.gov/privacy.

[6] At the time of completing this PIA, GRS 5.6 Security Records was still being finalized. ISMS will follow the retention guidelines that are finalized by NARA.

[7] For more information about IDMS, please *see* DHS/ALL/PIA-014 Personal Identity Verification/Identity Management System (PIV/IDMS) *available at* https://www.dhs.gov/privacy. For specific information about the IDENT/IDMS connection, please see DHS/ALL/PIA-014(b) Personal Identity Verification (August 23, 2012).

[8] For more information about the connection between ISMS and IDMS, please *see* DHS/ALL/PIA-038 Integrated Security Management System (March 22, 2011), *available at* https://www.dhs.gov/privacy

polygraph case number, polygraph type, polygraph agency, polygraph location, requestor, date requested, date scheduled, date of polygraph, polygraph results, date of results, and comments, along with other information listed below.

*Data Related to Work Email Address*

The ISMS record for an individual may contain the work email address for that individual. The work email address is located on the position record and is used by personnel security specialists to contact the subject when reinvestigations are due or for other personnel security-related matters.

# Privacy Impact Analysis

### Authorities and Other Requirements

The following is a list of authorities not previously identified in the original March 2011 ISMS PIA or subsequent PIA updates:

- 5 Code of Federal Regulations (CFR) Part 1400, "Designation of National Security Positions;"
- Executive Order (E.O.) 13488, "Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust;"
- E.O. 13549, "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities;"
- E.O. 13764, "Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters;"
- 5 CFR Part 736, "Personnel Investigations;"
- 6 CFR Part 7.10, "Authority of the Chief Security Officer, Office of Security;"
- Intelligence Community Policy Guidance (ICPG) Number 704.3, "Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes;"
- Homeland Security Presidential Directive-12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors;"
- DHS Policy Directive 121-04, "Security Clearance Reciprocity;"

- DHS Directive 121-01, "Chief Security Officer;" and
- DHS Instruction 121-01-007-01, "The Department of Homeland Security Personnel Security, Suitability, and Fitness Program."

## Characterization of the Information

*Data Related to IDENT Encounters*

- Encounter ID - an IDENT-generated number that is created each time an individual's biometrics are enrolled in IDENT;
- Encounter date - the date and time that the encounter activity was performed;
- Watch list code - provides a high level summary of the attention that should be given to an individual;
- Activity category - an enumerated list of types of encounter activities (*e.g.*, a visa application, a person entering at a Port of Entry);
- Activity reason - a free-text description of the encounter activity being performed;
- Originating organization - identifies the organization that originated the encounter;
- Encounter name - identifies the name of the encounter subject provided at the time of the encounter; and
- Encounter birth date - identifies the date of birth of the encounter subject.

*Fingerprint result information may be recorded in ISMS to include:*

- Date fingerprint was taken;
- Date fingerprint sent;
- Date result received;
- Transaction control number;
- Transaction reference number;
- FBI Fingerprint Identification Number (FIN);
- State identification number;
- Fingerprint result; and
- Fingerprint result (attachment).

*Data Related to Polygraph Events*

- Polygraph case number;
- Polygraph type;
- Security Office Identifier of administering agency;
- Polygraph agency;
- Polygraph location;
- Polygraph requestor;
- Date requested;
- Date scheduled;
- Date of polygraph;
- Polygraph result value;
- Date of results; and
- Remarks log.

The work email address for active employees and contractors is provided by the DHS Office of the Chief Human Capital Office (OCHCO) via Secure File Transfer (SFTP). The OCHCO file contains the ISMS position handle and the work email address. The ISMS position handle is a system-generated value that uniquely identifies a position. ISMS supports a data structure whereupon each "individual" may have multiple positions, and the Position Handle is used to uniquely identify a position associated with the individual. The ISMS position handle is used to match the work email address to the ISMS record.

**Privacy Risk:** There is a risk that ISMS may now be collecting more information than is necessary and relevant to accomplish its personnel security, administrative security, and classified visit management functions.

**Mitigation:** ISMS is responsible for a broad range of functions, thus it is necessary to maintain a large amount of information. The personally identifiable information (PII) maintained in ISMS consists of data elements necessary to identify the individual and to perform and track background investigations and other security related processes concerning the individual. The type of information collected from individuals and stored in ISMS will be dependent on the reason. For example, not all individuals will have their polygraph information maintained in ISMS. This information will be maintained in ISMS only if their position requires the completion of a polygraph as part of the personnel security adjudication process.

Additionally, in order to prevent misuse of the sensitive information in ISMS, access to the system is role-based, and data is only accessible if a specific user has been approved for access to the data. ISMS user accounts are individually approved by DHS Office of Security Division Chiefs before they are provisioned. All ISMS users must also have received DHS computer security training.

**Uses of the Information**

ISMS is used to store and maintain PII necessary to identify an individual and to track completion of suitability and security related processes, including background or other investigations concerning the individual.

Biometric encounter information, received from IDMS via IDENT, is used to assist in the DHS periodic reinvestigation process and continuous evaluation program.

Fingerprint result data is used to assist DHS in the fitness, suitability, reinvestigation, and continuous evaluation processes.

Polygraph data is used to assist DHS in the fitness and suitability processes.

Work email address is used to communicate via email with an individual on his or her personnel security or reinvestigation matters.

**Notice**

There have been no changes from the original March 2011 PIA and subsequent updates.

**Data Retention by the Project**

In response to NARA's ongoing update to GRS 18 with GRS 5.6, Security Records, ISMS plans to adhere to the finalized retention schedule.[9] The proposed retention schedules for ISMS data are listed below. These ISMS data retention changes are planned to support DHS's business use.

*Personnel Security Case Records*

DHS plans to mark for removal records of the agency's adjudication process and final determination that were created to conduct suitability, fitness, or security clearance determinations seven (7) years after the employee or contractor relationship ends. Seven years is the period of reciprocally accepting investigations and/or clearances and is the period required by Intelligence

[9] The original ISMS PIA from 2011 stated that FEMA would follow a different retention schedule. FEMA will now follow GRS 5.6 when it is finalized.

Community Policy Guidance (ICPG) 704.5 for retaining records on clearance holders where the clearance has been revoked or denied.

*Investigative Reports*

DHS plans to mark investigative reports for removal that were created to conduct suitability, fitness, or security clearance determinations based on the entity that created the investigative report (*i.e.*, investigation provider):

- **DHS Investigative Reports created under Office of Personnel Management (OPM) Delegated Authority** shall be marked for removal 20 years after receipt of the investigative report. The DHS Records and Information Management (RIM) Office has submitted a Department-wide records schedule to NARA that will supersede old job citations across the Department. In this retention schedule, personnel security investigations are destroyed/deleted 20 years after separation.
- **OPM/National Background Investigations Bureau (NBIB) or Other Agency Investigative Reports** shall be marked for removal when the investigative record meets the personnel security and access clearance records outlined above (seven years).

**Privacy Risk:** Because there is currently no established retention schedule, ISMS is retaining records permanently, creating the risk of ISMS retaining records for longer than is needed.

**Mitigation:** This risk is not currently mitigated. However, ISMS plans to follow the NARA-approve retention schedule once it is finalized.

**Privacy Risk:** There is a risk that the data will be retained beyond the record retention schedule once NARA establishes the requirements.

**Mitigation:** This risk is not currently mitigated. Archiving functionality will be used to ensure that information is removed from ISMS in accordance with the applicable retention schedule. Archiving allows for an individual's record to be placed in an archived file seven years after he or she departs DHS. The archived file can be manually reviewed to determine if the record should be purged in accordance with the records retention schedule. ISMS system administrators are able to adjust the archiving time period to ensure that retention of records in ISMS comply with the NARA-approved retention schedule.

## Information Sharing

ISMS is consuming new data from IDMS. However, the connection and transfer of other data between the two systems is not new.

**Redress**

There have been no changes from the original March 2011 PIA and subsequent updates.

**Auditing and Accountability**

There have been no changes from the original March 2011 PIA and subsequent updates.

## Responsible Official

Rosemarie Lawler
Deputy Chief, Enterprise Security Services Division
Management Directorate, Office of the Chief Security Officer
Department of Homeland Security

## Approval Signature

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

_____

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