Privacy Impact Assessment
for the

Integrated Security Management System (ISMS)

March 22, 2011

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

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Integrated Security Management System (ISMS) is a web-based case management tool designed to support the lifecycle of DHS personnel security, administrative security, and classified visit management[1] programs. Personnel security records maintained in ISMS include suitability and security clearance investigations which contain information related to background checks, investigations, and access determinations. For administrative security and classified visit management ISMS contains records associated with security container/document tracking, classified contract administration, and incoming and outgoing classified visitor tracking. The system is a DHS enterprise-wide application that replaced the Personnel Security Activities Management System, which was decommissioned on May 31, 2010.

Overview

In April 2008, the DHS Office of the Chief Security Officer (OCSO) implemented a web-based software solution to manage DHS personnel and administrative security case records across the DHS security enterprise. This enterprise system, known as ISMS, has replaced the existing personnel security case management system in use by DHS Headquarters, as well as systems at Customs and Border Protection (CBP), U.S Citizenship and Immigration Services (USCIS), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Center (FLETC), and U.S. Immigration and Customs Enforcement (ICE). The Transportation Security Agency (TSA) and the United States Coast Guard (USCG) are scheduled to transition to ISMS in fiscal year 2011.

ISMS provides a common repository for personnel security records across DHS 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). As a consolidated system, ISMS reduces the number of discrete interfaces that must be established and maintained 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 to include capturing the data related to suitability determinations, background investigations, security clearance processing, security container/document tracking, contract administration, and incoming/outgoing classified visitor tracking. The records in this system reflect the tracking/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.

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

[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.

the systems' data; or (c) access to national security information including classified information. Also covered are: 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.

The Personally Identifiable Information (PII) contained in this system consists of data elements necessary to identify the individual and to perform and track background investigations and other security related processes concerning the individual.

ISMS data is used internally by DHS with the exception of data sharing requirements related to employment eligibility, clearance verification associated with the classified visitor management program, and the transfer of relevant PII to the Office of Personnel Management (OPM), the Scattered Castles Secure Compartmented Information (SCI) database, and the Personal Identity Verification (PIV) Management System for the Homeland Security Presidential Directive 12 (HSPD-12) system.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

The interests of national security require that all persons privileged to be employed or work as a contractor in the departments and agencies of the government shall be reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States. This means that employment in any department or agency of the government is subject to investigation.

The U.S. Government conducts background investigations to determine if applicants or employees meet the suitability or fitness requirements for employment, or are eligible for access to federal facilities, automated systems, or classified information. The requirement to be investigated applies whether or not the position requires a security clearance (in order to have access to classified national security information). The scope of the investigation will vary, depending on the nature of the position and the degree of harm that an individual in that position could cause.

DHS maintains the results of the required background investigations in ISMS in accordance with the following Executive Orders and regulations:

(1) Executive Order (EO) 9397, Numbering System for Federal Accounts Relating to Individual Persons, as amended by EO 13478, Amendments to EO 9397 Relating to Federal Agency Use of Social Security Numbers.

(2) EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information.

(3) EO 10577, Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service.

(4) Title 5, Code of Federal Regulations, Part 731, Suitability;

(5) Title 5, Code of Federal Regulations, Part 732, National Security Positions;

(6) The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, codified in Executive Order 13381 (6-27-05). The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, codified in Executive Order 13381, 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 here directly supports this mandate.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The following Privacy Act SORNs apply to ISMS:

Department of Homeland Security/All-023 Personnel Security Management System of Records, Federal Register: February 23, 2010 (Volume 75, Number 35, pages 8088-8092); and

Department of Homeland Security/All-024 Facility and Perimeter Access Control and Visitor Management System of Records, Federal Register: February 3, 2010 (Volume 75, Number 22, pages 5609-5614).

1.3 Has a system security plan been completed for the information system(s) supporting the project?

A System Security Plan has been completed for ISMS, and a security certification authorizing the Authority to Operate (ATO) was granted on April 21, 2008, by the DHS Information Systems Security Manager Certifying Official. The ISMS Federal Information Security Management Act (FISMA) ID is ISD-03501-MAJ-03501.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

DHS adheres to NARA General Records Schedule 18, Security and Protective Services Records, items 21 through 25 for the retention schedule of personnel security clearance records. FEMA has approved schedules for FEMA series SEC-38-2-1 and SEC-38-2-1 under authority N1-311-94-1.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

OMB control numbers for information covered by the PRA are:

1. Standard Form 86, Questionnaire for National Security Positions, OMB No. 3206-0005;

2. Standard Form 85P, Questionnaire for Public Trust Positions, OMB No. 3206-0191; and

3. Standard Form 85, Questionnaire for Non-Sensitive Positions, OMB No. 3206-0005.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Information contained in ISMS is collected directly from covered individuals to 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. Also covered are: State and local government personnel and private-sector individuals who serve on an advisory committee or boards sponsored by DHS, or who need 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.

The Personnel Security (PERSEC) module within ISMS is used to store and maintain PII necessary to identify an individual and to track completion of suitability and personnel security related processes, including background or other investigations concerning the individual.

The following information is collected to identify a covered individual and support the suitability and security clearance process:

- Full Name
- Social Security Number (SSN)
- Address
- Date of Birth
- Place of Birth

- Citizenship Country
- Eye Color
- Hair Color
- Height
- Weight
- Gender
- Race
- Duty Location
- Employee Type
- Organization/Division
- Position Title
- Position Sensitivity
- Clearance Level
- Date Questionnaire for National Security or Non-Sensitive Positions and required signed certification forms received
- Date Fingerprint results received from FBI
- Date Credit Check completed
- Date National Crime Information Center (NCIC) Check was completed
- Type of Background Investigation required
- Date Background Investigation completed
- Date Approved to Enter-on-Duty
- Final Suitability and Security Clearance determination
- Collateral Clearance and Sensitive Compartmented Information (SCI) certification dates including brief & debrief dates
- Security Training dates
- Briefing Dates (SF-312 – Classified Information Non-Disclosure Agreement, Security, Education, Training and Awareness (SETA), SCI)
- Self-Reported Foreign Travel
- Self-Reported Foreign Contacts

Results from the background checks (e.g., credit, fingerprint, NCIC), the background investigation, and other personnel related data including but not limited to position, grade, series, step, and pay plan may be stored in ISMS. This information is stored in order to centralize case related documents and to shorten review and approval times associated with case processing.

In addition to the PERSEC module, ISMS also includes separate modules to support information security (INFOSEC), contract data collection (CONTACT), and classified visit management (VISIT).

The INFOSEC module supports the identification of DHS facilities and allows for the identification and tracking of storage containers and documents. The module integrates with the PERSEC module to indicate responsible container and document owners.

The Contract module is intended to collect data on DHS contract companies, contracts, and/or task orders. The module integrates with the PERSEC module by generating a valid list of companies, contracts, and/or task orders that can be assigned to contractor records. The VISIT

module is intended to support the tracking of incoming and outgoing classified visit requests from/to other U.S. Government Agencies. The outgoing visit request feature integrates with PERSEC by indicating the investigation level, clearance level, and special program access authorizations (if applicable) for DHS persons visiting a non-DHS government facility. The incoming visit request feature is used to collect PII necessary to identify the individual visiting DHS and to track security related information for access to DHS facilities or program information. The ISMS VISIT module stores the following information for visitors to DHS involving the exchange or discussion of classified information:

- Full Name
- SSN
- Date of Birth
- Place of Birth
- Citizenship Country
- Employee Type
- Organization
- Security Investigation types & date(s) completed
- OPM investigation scope

The ISMS application does not create any score or perform analysis of data.

Personnel Security Specialists import information into ISMS from the following systems:

- DHS Applicant Data – DHS Personnel Security Specialists have the option of downloading PII from OPM's Electronic Questionnaire for Investigations Processing (e-QIP) as an individual XML file. The file includes: SSN, last name, first name, middle initial, birth date, birth state, birth country, home address, home phone, work phone, gender, height, and weight. The information is used to create or update an individual's record.

- DHS Employee Data - A monthly encrypted batch file is provided by DHS Office of the Chief Human Capital Officer on DHS federal employees. The file includes: SSN, Position Number, last name, first name, middle initial, position sensitivity, agency, birth date, duty date, gender, pay plan series, occupation series, grade, and position title. The information is used to verify person and position data and to maintain the status of the employee position as active or inactive.

- Investigation Status – DHS Personnel Security Specialists access the OPM Personal Investigation Processing System (PIPS) and create a weekly file extract containing the status of background investigations currently being performed by OPM for DHS. The file includes: SSN, Case Number, last name, first name, middle initial, birth date, birth place, investigation type, investigation schedule date, investigation status, and an issue code for completed cases. The information is used to maintain the status of investigations ordered by DHS.

2.2 What are the sources of the information and how is the information collected for the project?

Personnel suitability/security request forms are used to initiate data collection. These forms are completed by DHS Human Capital offices, Contract Officers (COs), and/or Contractor Officer Technical Representatives (COTRs). Additional information is then collected directly from the covered individual electronically via the OPM electronic e-QIP system. E-QIP automates the "Questionnaire for Public Trust Positions" (SF-85P) and the "Questionnaire for National Security Positions" (SF-86) forms.

Other sources of information include:

Credit Checks – Credit reports are requested from commercial data providers. ISMS tracks the date the credit authorization was signed by the individual, the date the credit report was requested by DHS and the date the credit report was received by DHS. Personnel Security Specialists have the option of attaching a copy of the credit report to the ISMS record or storing the report in paper form in the individual's personnel security folder. ISMS maintains the source of the credit check via the credit report if attached to the ISMS record.

Fingerprint Checks – Fingerprint checks are submitted and verified using the FBI Integrated Automated Fingerprint Identification System (IAFIS). ISMS tracks the date when the fingerprint check was requested and the date the result was received. Personnel Security Specialists have the option of attaching a copy of the fingerprint results to the ISMS case or storing the results in paper form in the individual's personnel security folder.

Suitability Investigations Index (SII)/Clearance Verification System (CVS)/Joint Personnel Adjudication System (JPAS) Check – Previously conducted investigations, clearances, polygraphs, and adjudications for a given individual are collected/verified using the OPM CVS. ISMS tracks the date of when the SII/CVS/JPAS check was completed, and allows for the entry of the date and type of prior investigations, clearances, or polygraphs identified in SII/CVS/JPAS. Personnel Security Specialists have the option of attaching a copy of the screen displays to the ISMS record or storing the results in paper form in the subject's personnel security folder.

Citizenship and Immigration Services (CIS) Check – The USCIS Central Index System (CIS) database is checked to verify the U.S citizenship of an applicant and the U.S. citizenship or the immigration status of reported foreign born immediate family members. The CIS database is used because it contains expanded information on the type of visa the individual has been issued as well as information on any special circumstances associated with the issuance of the visa. The search is conducted by entering the exact name and date of birth of a subject. If a match is found, the system displays a screen with citizenship status in the Class of Admission (COA) field. ISMS tracks the date when the CIS check was conducted. Personnel Security Specialists have the option of attaching a copy of the CIS screen result to the ISMS case or storing the results in paper form in the subject's personnel security folder.

TECS/National Crime Information Center (NCIC) Check. Law enforcement information, criminal history records, or outstanding warrants for a given individual are collected/verified

using TECS/NCIC. A DHS Personnel Security Specialist accesses NCIC through the TECS database, so these checks are conducted simultaneously. The search is conducted by entering the exact name, date of birth, and SSN of a subject. If a match is found the system displays a list of records, if no match is found, the system displays a screen indicating No Match Found. ISMS tracks the date when the TECS/NCIC check was completed. Personnel Security Specialists have the option of attaching a copy of the TECS/NCIC results report to the ISMS case or storing the results in paper form in the subject's personnel security folder.

Intelligence Community Security Clearance Repository (e.g., Scattered Castles) Check – A check of the Scattered Castles database is required for individuals who require access to Sensitive Compartmented Information (SCI). The Scattered Castles database is the U.S. Intelligence Community's authoritative personnel security repository for verifying personnel security access approvals regarding SCI and other controlled access programs, visit certifications, and documented exceptions to personnel security standards. ISMS tracks the date when the Scattered Castles check was completed. Personnel Security Specialists have the option of attaching a copy of the Scattered Castles results to the ISMS case or storing the results in paper form in the subject's personnel security folder.

Background Investigations – Background investigations are conducted by OPM or by DHS components when OPM has delegated authority (e.g., ICE and CBP) from OPM to conduct background investigations. At the conclusion of the investigation, a Report of Investigation (ROI) is submitted to DHS along with copies of the checks conducted during the investigation. ISMS tracks the investigation source, type, request date, schedule date, status, close date, and an issue code for completed investigations. Personnel Security Specialists have the option of attaching a copy of the Background Investigation to the ISMS case or storing the results in paper form in the subject's personnel security folder.

Classified visitor management information is manually entered by DHS Customer Service Center personnel (for classified visits) and by Special Security Programs Division (for those requiring special access(es)). Lastly, information pertaining to contracts which will involve working with classified materials is entered in the Contracts module[2] by the DHS/OCSO Administrative Security Division (ASD).

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

Credit Checks – Credit reports are requested from commercial data providers. ISMS tracks the date the credit authorization was signed by the individual, the date the credit report was requested by DHS and the date the credit report was received by DHS. Personnel Security Specialists have the option of attaching a copy of the credit report to the ISMS record. ISMS maintains the source of the credit check via the credit report if attached to the ISMS record.

[2] No classified material is entered in ISMS.

2.4 Discuss how accuracy of the data is ensured.

As part of the application process, the individual is required to enter their PII and background information into the OPM e-QIP system. The DHS OCSO, Personnel Security Division (PSD) receives the information from applications provided by the individual in the security clearance vetting or suitability review process. PII for federal employees is verified by comparing employee data against National Finance Center (NFC) reports provided by the DHS Office of the Chief Human Capital Officer (OCHCO). In addition, the PII provided by the individual is verified by the information collected during the FBI fingerprint check, credit check, NCIC check, FBI name check, OPM background investigation and other investigation(s) as deemed necessary based on suitability or national security investigation requirements.

As part of the classified visit process, the individual is required to provide their PII to their appropriate DHS point of contact who then manually enters the information into ISMS or who sends the information to the appropriate DHS OCSO division. The accuracy of that information is verified by the government agency which holds the individuals security clearance.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk associated with the accuracy of data included in the ISMS system. Although most of the PII data is generated by the individual it is possible that data associated with individuals with the same name or similar names could be inaccurately entered into ISMS.

There is also a risk associated with the wrong data being attached to an ISMS record or inserted into an incorrect personnel security folder.

Mitigation: To address potential occurrences of data being inaccurately entered into ISMS or inserted into an incorrect personnel security folder, the following mitigation strategies are used:

Electronic data collection tools are used to the greatest extent possible;

Records that are attached to the ISMS record or inserted in the personnel security folder include the subject's personally identifying information directly on the record. This information can be used to verify the correct subject;

There is a comprehensive vetting or suitability review process used for verifying accuracy of information; and

Redress opportunities are available to the individual as outlined in the SORN - Department of Homeland Security/All - 023 Personnel Security Management System of Records, 74 Federal Register 3084, published on January 16, 2009).

Section 3.0 Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses 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.

As described in section 2.1, PII collected to clearly identify an individual in order to begin and track the suitability or security clearance process(es) includes:

- Full Name
- SSN
- Date of Birth
- Place of Birth
- Citizenship Country
- Gender
- Employee Type
- Organization
- Position Sensitivity (determines the level of investigation required and/or if a security clearance is required).

Information required for Suitability and/or Security Clearance processing includes;

- Date Questionnaire for National Security or Non-Sensitive Positions and required signed certification forms received
- Date Fingerprint results received from FBI
- Date Credit Check completed
- Date National Crime Information Center (NCIC) Check was completed
- Type of Background Investigation required
- Date Background Investigation completed

Other Information maintained includes the outcome and timeframes that adjudication decisions were made in order to bring someone onboard or grant them access to DHS facilities and/or IT systems. This includes:

- Date Approved to Enter-on-Duty
- Final Suitability and Security Clearance determination
- Collateral Clearance and SCI certification dates including brief & debrief dates
- Briefing Dates (SF-312, SETA)
- Self-Reported Foreign Travel (required for TS/SCI clearance holders)
- Self-Reported Foreign Contacts (required for TS/SCI clearance holders)

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

Data in ISMS is used to track security related information and processes. There are no in-built data analysis functions to identify patterns or new areas of concern.

3.3 Are there other components with assigned roles and responsibilities within the system?

ISMS is used by security offices at DHS Headquarters, CBP, USCIS, FEMA, FLETC, and ICE. The data stored and managed by ISMS is partitioned by DHS 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. This includes the following OCSO Divisions: PSD, Customer Service Center (CS), Special Security Programs (SSPD), Physical Security (PHYSEC), and the OCHCO. These individuals, by law and contract, are bound by the Privacy Act. Specific information about an individual will be shared with Department employees and its contractors who have a "need to know" regarding the personnel security vetting process. Department contractors are contractually obligated to comply with the Privacy Act in the handling, use, and dissemination of PII.

OCSO PSD has access to the PERSEC module and uses ISMS data to process and adjudicate suitability and security clearance cases. CS has access to the PERSEC and VISIT modules and uses ISMS information to respond to individual's inquiries on the status of their applications and/or security clearance. SSPD has access to the PERSEC and VISIT modules and uses ISMS as a means to process and grant requests for access to SCI as well as process incoming visit requests for non-DHS persons holding TS/SCI clearances visiting DHS facilities. PHYSEC has limited access to the PERSEC module and uses ISMS to verify HSPD-12 PIV card requests; and OCHCO has limited access to the PERSEC module and uses ISMS data to make hiring decisions.

Access to ISMS data is via an authenticated web interface. Access control is role-based and data is only accessible if a specific user has been approved for access to the data. Information presented on screens is defined based on specific roles and information required to facilitate those functions.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There are privacy risks associated with the handling of PII that occur when data is extracted from the system and the individual using the data improperly distributes or stores the data.

Mitigation: To address these risks the following controls and mitigation strategies are in place:

- Handling of PII
    - A Data/Report request form must be completed, signed, and approved by the requester, requester's manager and the Chief, Personnel Security Division prior to the creation and/or distribution of personnel security data, to avoid accidental, inappropriate or unauthorized use of the data;
    - Access to information is granted on a "need to know" basis;
    - Access to ISMS requires a DHS domain account and requires that the user be logged into a DHS Intranet accessible computer;
    - ISMS user accounts are individually approved by DHS Office of Security Division Chiefs before they are provisioned;
    - All users have received DHS Computer Security training and have been vetted and/or cleared for access to privacy, sensitive, and/or classified information;
    - Access to ISMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access;
    - The DHS Privacy Office has prepared and published the Handbook for Safeguarding Sensitive Personally Identifiable Information; and
    - Write capability, which is limited to a few roles, is tracked and audited.

Privacy Risk: There are privacy risks associated with system security that concern an "insider threat" where an individual authorized access to the system conducts unauthorized activities, e.g., attempting to access information for which they do not have permission.

Mitigation: To address these risks the following controls and mitigation strategies are in place:

- System Security
    - When 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;
    - All automated data processing equipment supporting the application environment is located in a DHS data center;
    - Specific security roles have been defined and implemented within the application to control access to information;
    - A system security certification was performed and obtained in accordance with the Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources; and
    - Network access to the application is made via a Secure Sockets Layer (SSL) connection to the ISMS environment.

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

In all cases, individuals are provided notice required by the Privacy Act, 5 USC § 552a. The Privacy Act statement, as required by the Privacy Act, 5 USC § 552a(e)(3) states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used. The collection, maintenance, and disclosure of information complies with the Privacy Act and the published the DHS/ALL-023 Personal Security Management SORN, 74 FR 3084, published January 16, 2009. The Standard Forms used for data collection have OMB approved Privacy Act statements.

Individuals confirm in writing that they have been presented and are in agreement with the Privacy Act statement and agree to participate in the suitability and clearance process and submit to a named-based threat background check appropriate to job requirements.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Individuals may opt to not provide information; however, if the information is not provided they will not meet suitability requirements and will be ineligible for federal employment. Furthermore, if information is not provided they are ineligible to serve a role as a government contractor at a federal facility for a period of more than six months. Individuals waive the right to choose how the information will be used on submission of the SF-85 or SF-86.

Individuals are notified of the uses of their information prior to collection. Once the information is provided the individual has given consent to the uses. The DHS OCSO will not use the information outside of the scope of this PIA and the SORN. Should a new use for the information be foreseen the PIA and/or the SORN will be updated.

4.3 Privacy Impact Analysis: Related to Notice

There is no privacy risk associated with individuals being provided privacy-related notice. Individuals are provided with privacy notices and statements on the forms used to collect the information. Additionally, the SORN and this PIA provide additional notice of the collection, use, maintenance, and dissemination of and individual's PII.

Section 5.0 Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

DHS Personnel Security Records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, items 22 through 25, approved by NARA.

Personnel Security Clearance Files

Case files documenting the process of investigations to include: questionnaires, summaries of reports prepared by the investigation agency, and other records reflecting the processing of the investigation and the status of the investigation. Disposition: Destroy upon notification of death or not later than five years after separation or transfer of employee or no later than five years after contract relationship expires.

Case files relating to investigations of alleged violations of Executive Orders, laws, or agency regulations for the safeguarding of nation security information. Disposition: Destroy five years after close of case.

Classified Information Nondisclosure Agreements

Copies of nondisclosure agreements such as SF 312, Classified Information Nondisclosure Agreement, signed by employees with access to information that is classified under standards put forth by Executive orders governing security classification. Disposition: Maintained with the individual's official personnel folder and follows the disposition schedule of the official personnel folder.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: A risk associated with the retention of information is that the data will be retained beyond the requirements established in the record retention schedule.

Mitigation: An archiving application in the ISMS Personnel Security Module is being used to ensure that information is removed from the ISMS system in accordance with records retention schedules. The archiving application allows for an individual's record to be placed in an archived file when they depart DHS. The archived file can be manually reviewed to determine when the record should be purged in accordance with the record retention schedule.

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities.

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Information is shared to facilitate security clearance reciprocity and access to controlled facilities. Clearance information is shared with OPM; U.S. Intelligence Community; HSPD-12 Identity Management System (IDMS) in order to facilitate issuance of PIV cards in support of HSPD-12; and the ICE/USCIS PERSECS system that ultimately grants Information Technology access levels to ICE/USCIS personnel.

Background investigation, and clearance verification and eligibility information as well as relevant personal data will be shared with:

1. OPM Clearance Verification System;
2. U.S. Intelligence Community SCI database when needed/appropriate. SCI clearance status information including clearance eligibility dates, personnel type, organization, clearance level and SCI certification dates is shared;
3. PIV Management System, IDMS for the Homeland Security Presidential Directive 12 (HSPD-12) system;
4. ICE/USCIS PERSECS that ultimately sends out IT access levels that ICE/USCIS personnel have been granted via ISMS; and
5. Authorized organizations which require access to security clearance information, in conformance with the SORN, Personal Identity Verification Management System (PIVMS), DHS-OS-002, published on September 12, 2006, 71 FR 53697.

This information is shared as necessary to facilitate National Security Clearance reciprocity, access to controlled facilities, and issuance of PIV cards in support of HSPD-12.

Information about individuals that is stored for purposes of granting clearances may be given without individual's consent as permitted by the Privacy Act of 1974 (5 U.S.C. § 552a(b)), including to an appropriate government law enforcement entity if records show a violation or potential violation of law.

Information may also be shared with federal, state, or local law enforcement or intelligence agencies or other organizations in accordance with the Privacy Act and the routine uses identified in the Personnel Security Management System of Records.

The following PII maintained in ISMS is shared to facilitate security clearance

reciprocity, access to controlled facilities, access to ICE/USCIS IT systems, and issuance of PIV cards in support of HSPD-12:

- Full Name;
- SSN;
- Date of Birth;
- Security Clearance level;
- Clearance eligibility dates;
- Other information as defined by OPM to facilitate security clearance reciprocity requirements for personnel who hold security clearances.

The following PII maintained in ISMS is shared with the U.S. Scattered Castles system:

- Full Name;
- SSN;
- Date of Birth;
- Organization;
- Security Clearance level;
- Clearance Eligibility Dates;
- Personnel Type;
- SCI Clearance certification dates including brief & debrief dates.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

All routine uses discussed in Section 6.1 above are compatible with the SORN (Department of Homeland Security/All—023 Personnel Security Management System of Records, Federal Register: February 23, 2010 (Volume 75, Number 35, pages 8088-8092) as described on page 8091 are pursuant to 5 U.S.C. 552a(b)(3).

6.3 Does the project place limitations on re-dissemination?

Background investigations conducted by OPM are not shared with external agencies. External agencies must request background investigations from the agency which conducted the investigation.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

As identified in the DHS/ALL-023 Personal Security Management SORN, 74 FR 3084,

published January 16, 2009, requests for personnel security information are made to the DHS Freedom of Information Office (FOIA) who maintains the accounting of what records were disclosed and to whom. The DHS FOIA office submits a request for information to the DHS Personnel Security Division. The PSD has the option of using the ISMS File Request module to track FOIA office requests.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that the user will violate the no onward transfer policy.

Mitigation: To address this risk the following controls are in place:

- A Data/Report request form must be completed, signed, and approved by the requester, requester's manager and the Chief, Personnel Security Division prior to the creation and/or distribution of personnel security data, to avoid accidental, inappropriate or unauthorized use of the data;
- Access to information is granted on a "need to know" basis;
- Access to ISMS requires a DHS domain account and requires that the user be logged into a DHS Intranet accessible computer;
- ISMS user accounts are individually approved by DHS Office of Security Division Chiefs before they are provisioned;
- All users have received DHS computer security training and have been vetted and/or cleared for access to privacy, sensitive, and/or classified information;
- Access to ISMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access; and
- Write capability is limited to a few roles, is tracked and audited.

Section 7.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals to access their information?

ISMS stores PII, suitability, and security clearance process tracking information related to an individual. The information is self-reported by the individual undergoing a background investigation when they submit their completed SF-85 / SF-86 or e-QIP entry. Individuals are able to correct erroneous information in e-QIP before submission. Once that data has been submitted to ISMS for suitability review and clearance processing, individuals must contact either PSD or Customer Service directly, or go through Privacy/FOIA Office to gain access to their PII.

Each individual has the ability to address and provide mitigating information related to any derogatory information that is identified as part of his/her background investigation. Subjects are notified of any pending actions based on derogatory information and are provided a

mechanism to provide information. If a derogatory finding is made, they have appeal rights, and also the ability to request information regarding their case via the DHS FOIA office.

As identified in the DHS/ALL-023 Personal Security Management SORN, 74 FR 3084, published January 16, 2009, requests for personnel security information are made to the DHS FOIA Office which maintains the accounting of what records were disclosed and to whom. The DHS FOIA Office submits a request for information to the DHS PSD. The PSD has the option of using the ISMS File Request module to track FOIA office requests.

Privacy Act requests for access to an individual's record must be in writing and may be addressed to the DHS FOIA/PA, The Privacy Office, U.S. Department of Homeland Security, 245 Murray Drive SW, STOP-0550, Washington, DC 20528-0550

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Information in ISMS is obtained as a data extract from e-QIP from data provided directly by the individual. Accuracy of an individual's data is checked by an investigation; a PSD security assistant then reviews the results.

The specific procedures for an individual to view and request changes depend on the findings and the type of case. Subjects are notified in writing when DHS is prepared to make a derogatory finding based on the information at hand. The written notice advises the individual of the mechanism for addressing the derogatory information.

7.3 How does the project notify individuals about the procedures for correcting their information?

The specific procedures depend on the findings and the type of case. Individuals are notified in writing when DHS is prepared to make a derogatory finding based on the information available to DHS. The written notice advises the individual of the mechanism for addressing the derogatory information. The individual will be notified based on a review of their response whether the derogatory information will result in a change to their suitability and/or clearance status. If their clearance is suspended or revoked, they will be notified in writing and be provided with the specific information regarding their appeal rights and due process. Additionally instructions are provided on related security forms regarding changes or updates to data that may be required after submission.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: A potential risk associated with redress concerns the ability to validate the accuracy of the information being revised. Most PII contained in ISMS is self-reported by the individual undergoing a background investigation when they submit their completed SF-85 / SF-86 or e-QIP entry. Individuals are able to correct erroneous information in e-QIP before submission.

Mitigation: Additional investigation and record checks (through Human Capital, National Finance Center, and other organizations) are conducted to validate the accuracy of information submitted through a redress process.

Section 8.0 Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Access to the information is via an authenticated web interface. Access control is role-based and data is only accessible if a specific user has been approved for access to the data. Information presented on screens is defined based on specific roles and information required to facilitate those functions. Permissions can be assigned to a specific role having either "read-only" or "edit" capability. Additionally, ISMS provides the ability to mark specific records as "Limited Access" and only those users with Limited Access privileges can view those records.

The system has auditing capabilities that stamps who, when, and what changes were made to a given record. If users attempt to view their own record, they are immediately logged out of the system and their accounts locked.

Periodic reviews are conducted on the application of user roles and administrative actions are conducted by the ISMS Support team.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All DHS employees and assigned contractor staff receive appropriate privacy and security training, and have undergone necessary background investigations and/or security clearances for access to sensitive, privacy, or classified information or secured facilities. DHS ensures this through legal agreements with its contractors and enforcement of internal procedures with all DHS entities involved in processing the background checks. Additionally, robust standard operating procedures and system user manuals describe in detail user roles, responsibilities and access privileges.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

ISMS user accounts are individually approved by DHS Office of Security Division Chiefs before they are provisioned;

All users must have received DHS computer security training and have been vetted and/or cleared for access to privacy, sensitive and/or classified information; and,

Access to ISMS is role-based: users of the system have access to a limited subset of data based on the concept of least privilege/limited access.

Procedures are documented in ISMS Administrative Guide and ISMS System Security Plan.

8.4 How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

ISMS establishes data sharing agreements with external entities using Interconnection Security Agreements (ISAs). DHS 4300A, Sensitive System Handbook, September 2008, establishes this requirement for DHS systems. An ISA is required whenever the security policies of the interconnected systems are not identical and the systems are not administered by the same entity/Designated Accrediting Authority (DAA). The ISA documents the security protections that must operate on interconnected systems to ensure that transmissions between systems permit only acceptable transactions. The ISA includes descriptive, technical, procedural, and planning information. It also formalizes the security understanding between the authorities responsible for the electronic connection between the systems. The DAA for each organization is responsible for reviewing and signing the ISA.

Responsible Officials

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

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security