Privacy Impact Assessment Update
for the

Integrated Security Management System (ISMS) – Continuous Evaluation

DHS/ALL/PIA-038(d)

September 16, 2019

Contact Point
Doug Ericson
Deputy Director, ISMS
Office of the Chief Security Officer
Management Directorate
(202) 447-0166

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 outline Continuous Evaluation (CE), which is part of overarching personnel security clearance reform efforts directed by Executive Order (E.O.) 13467, as amended by E.O. 13764, and Security Executive Agent Directive (SEAD) 6, issued by the Director of National Intelligence (DNI). Through this initiative, DHS will be sharing personally identifiable information (PII) of covered individuals with the Office of the Director of National Intelligence (ODNI) via ISMS.

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 and also provides the ability to shift personnel security resources from one DHS Component to another for surge support without incurring extensive retraining.

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

Reason for the PIA Update

DHS is updating this PIA to incorporate the sharing of PII of covered individuals[3] with

[1] Classified visit management is an administrative process in which an individual's security clearance information is exchanged between agencies to document an individual's security clearance level.
[2] Note that some Component personnel security divisions have the ability to manage contract or task order data in ISMS and then associate contractors to those contracts or task orders.
[3] SEAD 6, *available at* https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy,
defines "covered individuals" as:

ODNI as part of the Department-wide program for CE. The Director of National Intelligence, as the Security Executive Agent, issued Security Executive Agent Directive (SEAD) 6, which applies to any executive branch agency, authorized adjudicative agency, authorized investigative agency, and covered individuals. SEAD 6 directs that "CE shall be conducted on covered individuals with national security eligibility" and permits agencies to use the CE services provided by the National Counterintelligence and Security Center (NCSC) to meet this obligation.

The overall CE effort is led by NCSC on behalf of the Director of National Intelligence as the Security Executive Agent. NCSC provides oversight and guidance for implementing CE across the executive branch and is developing the Continuous Evaluation System (CES), a technical solution to conduct the automated records checks that are the core of CE. CES conducts automated records checks of commercial and government databases to flag security-relevant information, allowing for more frequent follow-up by security personnel of the appropriate agency.

Continuous Evaluation

The DHS CE Program is an integral part of reform efforts to modernize the personnel security process. The primary objective for the DHS CE Program is to develop an automated solution for continuous records checks on the eligible DHS population,[4] which delivers only the relevant potentially derogatory information, not previously adjudicated, to DHS personnel security offices for adjudication. CE is a means for reviewing the backgrounds of individuals on an ongoing basis to determine whether the individuals continue to meet applicable personnel security requirements.

(a) A person who performs work for or on behalf of the executive branch or who seeks to perform work for or on behalf of the executive branch, but does not include the President or (except to the extent otherwise directed by the President) employees of the President under 3 U.S.C. §§ 105 or 107, the Vice President or (except to the extent otherwise directed by the Vice President) employees of the Vice President under 3 U.S.C. § 106 or annual legislative branch appropriations acts;
(b) A person who performs work for or on behalf of a state, local, tribal, or private sector entity, as defined in E.O. 13549, but does not include duly elected or appointed Governors of a state or territory, or an official who has succeeded to that office under applicable law;
(c) A person working in or for the legislative or judicial branches with eligibility for access to classified information and the investigation or determination was conducted by the executive branch; but does not include Members of Congress; Justices of the Supreme Court; and federal judges appointed by the President; and
(d) Covered individuals are not limited to government employees and include all persons, not excluded under paragraphs (a), (b), or (c) of this definition, who require eligibility for access to classified information or eligibility to hold a sensitive position, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts, consultants, and government employees.

[4] The eligible DHS population that will be enrolled in the automated NCSC CES records checks is anyone in a national security position who has completed a Standard Form 86, "Questionnaire for National Security Positions," version 2010 or later. National security positions include any position in DHS which could cause significant damage to national security regardless of eligibility for access to classified information.

CE records checks supplement the existing investigative process by transforming personnel security investigations from periodic snapshots to ongoing reviews that bridge the information gaps within the reinvestigation cycle. This will help mitigate the risk posed by insiders who potentially represent a threat to national security through proactive intervention and identification of security-relevant information earlier so that the appropriate action can be taken.

DHS has opted to use the NCSC-established CES to conduct CE, in addition to leveraging existing DHS information systems. PII of covered individuals is extracted from ISMS and shared with NCSC as an encrypted file. NCSC then conducts automated records checks that will identify relevant information to assist DHS security personnel in assessing the continued eligibility of a covered individual on an ongoing basis during the period of eligibility. The automated records checks will include checks of commercial databases, U.S. Government databases, and other information lawfully available to NCSC security officials on an ongoing basis during the period of eligibility.[5] NCSC, through CES, will provide DHS personnel security officials with information that they will analyze to determine if the information is of a security concern for further investigation and adjudication.

Privacy Impact Analysis

Authorities and Other Requirements

The following is a list of applicable authorities not previously identified in the latest ISMS PIA dated June 26, 2017:[6]

- SEAD 3, "Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position;"[7]
- SEAD 4, "National Security Adjudicative Guidelines;"
- SEAD 6, "Continuous Evaluation;"
- SEAD 7, "Reciprocity of Background Investigations and National Security Adjudications;" and
- ODNI and Office of Personnel Management (OPM) Executive Correspondence, "Transforming Workforce Vetting: Measures to Reduce the Federal Government's Background Investigation Inventory in Fiscal Year 2018."

Characterization of the Information

No new information is being collected from DHS personnel as part of this initiative. The

[5] For more information about the CES process at NCSC, please *see* https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-continuous-evaluation-overview.
[6] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy.
[7] All published Security Executive Agent Directives, including 3, 4, 6, and 7 which are applicable to CE, are *available at* https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-security-executive-agent/ncsc-policy.

PII shared with NCSC is already maintained in ISMS and collected through the initial personnel security vetting and reinvestigation processes. This information is collected directly from DHS personnel generally via the Standard Form (SF) 86, "Questionnaire for National Security Positions." The below data elements will be shared with NCSC:

- Full name;
- Aliases;
- Gender;
- Date of birth;
- Place of birth;
- Citizenship;
- Social Security number;
- Current address(es);
- Previous address(es);
- Personal email address(es);
- Phone number(s); and
- Passport information.

Should potentially derogatory information be identified from records checks through CES, a new case with that information will be created by DHS personnel security officials in the subject's personnel security file within ISMS for further investigation and evaluation. If the records checks produce no results, no new case will be created in ISMS.

Privacy Risk: There is a risk that inaccurate information will be shared or used in the DHS CE Program.

Mitigation: This risk is mitigated. All information transferred to and from NCSC is encrypted in transit, which ensures that the information is not altered while it is being shared from ISMS. Additionally, information is safeguarded in accordance with recommended and prescribed administrative, physical, and technical safeguards while it resides in ISMS to ensure data integrity. Records are maintained in secure U.S. Government facilities with access limited to authorized personnel. Physical security protection includes guards and locked facilities requiring badges and passwords for access. Records are accessed only by authorized DHS and NCSC personnel whose official duties require access to the records.

ISMS itself has several mechanisms in place to ensure accurate data is shared with NSCS: 1) electronic data collection tools are used to the greatest extent possible as opposed to manual entry of data into ISMS; 2) OCSO has a comprehensive vetting or suitability review process used

for verifying accuracy of information; and 3) redress opportunities are available to all personnel as outlined in DHS/ALL-023 Personnel Security Management.[8] Additionally, DHS investigates any potentially derogatory information it receives against other sources of information, thereby mitigating the impact posed by inaccurate data from ISMS being used in records checks and thus producing inaccurate results.

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. DHS is continuing to use the information maintained in ISMS to track completion of suitability- and security-related processes.

Information from ISMS is also being shared with NCSC to perform records checks as part of the CE process. DHS personnel information will only be shared with NCSC for the purpose of CE. NCSC will not further share the information with any other federal department or agency. Information discovered as a result of a CE record check will only be shared with the department or agency that enrolled that individual into CE.

Notice

DHS will provide a Department-wide communication message that will outline the DHS CE Program, indicate who will be included in the CE process, and inform that consent to be included in a CE Program was granted by the individual signing an SF-86, "Questionnaire for National Security Positions," 2010 version or later.[9] This PIA also outlines the privacy impacts of DHS's implementation of CE.

Privacy Risk: There is a risk that personnel who joined the Department prior to 2010 are unaware of DHS's implementation of CE.

Mitigation: This risk is mitigated. Individuals are made aware of this CE process through this PIA and the Department-wide communication message. Additionally, all of the DHS personnel eligible for enrollment in the automated NCSC CES records checks have signed the SF-86, which informed them that they are eligible for CE. These records checks are part of the existing process of background investigations and reinvestigations, CE is just automating these records checks.

Privacy Risk: There is a risk that individuals may not be aware of how CE may affect

[8] DHS/ALL-023 Personnel Security Management, 74 FR 3084, (January 16, 2009).
[9] Individuals complete a Standard Form 86 in order for the U.S. Government to collect information for "conducting background investigations, reinvestigations, and continuous evaluations of persons under consideration for, or retention of, national security positions as defined in 5 CFR 732, and for individuals requiring eligibility for access to classified information under Executive Order 12968." For more information, please *see*: https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf.

them. For example, one of the records checks CE conducts is credit checks. An individual may not understand how a freeze he or she has placed on his or her credit reports impacts the records checks.

Mitigation: This risk is mitigated. DHS is publishing an online "*DHS Continuous Evaluation: What You Should Know*" information guide that explains what actions may be required of individuals and what other impacts CE may have, and specifically addresses credit checks.[10]

Data Retention by the Project

Pursuant to 44 U.S.C. 3303a(d) and 36 CFR 12, Subchapter B – Records Management, and as reflected in ODNI's System of Records Notice (SORN) for the Continuous Evaluation System,[11] PII of covered personnel stored in ISMS and shared with NCSC is covered by National Archives and Records Administration General Records Schedule 5.6, Security Records, items 170 through 181, and will be retained and disposed of according to those provisions.[12] As such, NCSC will generally destroy PII five years after the covered personnel relationship ends with DHS.

Information Sharing

DHS will share PII of covered personnel with NCSC for automated records checks using the NCSC CES. PII shared with NCSC will be encrypted in transit. The NCSC CE Program will only share CES alerts and reports with the sponsoring department that enrolled its personnel in the NCSC CES.

Privacy Risk: There is a privacy risk that the information shared by DHS is not properly handled and protected or is misused by the receiving agency.

Mitigation: This risk is mitigated. Pursuant to SEAD 6, NCSC is responsible for implementing technical and security safeguards to ensure CES protects the privacy, civil rights, and civil liberties of covered individuals. In addition, as articulated in ODNI's Continuous Evaluation System SORN, NCSC safeguards records in accordance with prescribed administrative, technical, and physical safeguards; all searches of the system will be performed by authorized executive branch security personnel; and any disclosures will be made consistent with the limitations in the SORN and SEAD 6.

Redress

There have been no changes from the original March 2011 PIA and subsequent updates. Each covered individual continues to have the ability to address and provide mitigating information related to any potentially derogatory information that is identified as part of his or her

[10] *See* http://dhsconnect.dhs.gov/org/comp/mgmt/ocso/ESOS/Pages/Continuous-Evaluation.aspx.
[11] ODNI/NCSC-003, 83 FR 61395 (November 29, 2018).
[12] *See* https://www.archives.gov/files/records-mgmt/grs/grs05-6.pdf.

CE process. Subjects are notified of any pending actions based on derogatory information and are provided a mechanism to provide additional explanatory or mitigating information. If a derogatory finding is made by DHS, individuals have appeal rights, and the ability to request information in accordance with the DHS/ALL-023 Personnel Security Management System of Records Notice.[13]

Auditing and Accountability

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

Responsible Official

Doug Ericson
Deputy Director, ISMS
Office of the Chief Security Officer
Department of Homeland Security

Approval Signature

Original, signed version on file with the DHS Privacy Office.

_____

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

[13] DHS/ALL-023 Personnel Security Management, 74 FR 3084, (January 16, 2009).