Privacy Impact Assessment
for the

DHS Insider Threat Program

DHS/ALL/PIA-052(a)

March 1, 2018

Contact Point
Sean Thrash
Insider Threat Program Manager
Office of the Chief Security Officer
202-447-5316a

Richard D. McComb
Senior Insider Threat Official
Chief Security Officer

Reviewing Official
Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Insider Threat Program (ITP) was established as a department-wide effort to manage insider threat matters within DHS. The Insider Threat Program was mandated by E.O. 13587, ''Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,'' issued October 7, 2011, which requires all federal agencies that operate or access classified computer networks, to establish an insider threat detection and prevention program covering all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), to ensure the security of classified networks and the responsible sharing and safeguarding of classified information on those networks with appropriate protections for privacy and civil liberties. Insider threats include: attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against the Department and its personnel, facilities, resources, and activities; unauthorized use of or intrusion into automated information systems; unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary information or technology; and indicators of potential insider threats. The DHS ITP monitors activity on all three DHS networks: Unclassified (A-LAN), SECRET (B-LAN also known as the Homeland Secure Data Network), and TOP SECRET (C-LAN also known as the Joint Worldwide Intelligence Communications System) for attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against the Department and its personnel, facilities, resources, and activities; unauthorized use of or intrusion into automated information systems; unauthorized disclosure of classified, controlled unclassified, sensitive,[1] or proprietary information or technology; and indicators of potential insider threats by covered persons.[2] DHS is updating this Privacy Impact Assessment (PIA) to reflect the application of the insider threat program to all networks.

[1] The Computer Security Act of 1987, Public Law 100-235, defines "sensitive information" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy."

[2] Covered individuals include: 1) DHS current or former employees, contractors, or detailees who have access or had access to sensitive or classified national security information; 2) Other individuals, including federal, state, local, tribal, and territorial government personnel and private-sector individuals, who are authorized by DHS to access departmental facilities, communications security equipment, and/or information technology systems that process sensitive or classified national security information; 3) Any other individual with access to sensitive or classified national security information who accesses or attempts to access DHS IT systems, DHS sensitive or classified national security information, or DHS facilities 4) Family members, dependents, relatives, and individuals with a personal association to an individual who is the subject of an insider threat investigation; and 5) Witnesses and other individuals who provide statements or information to DHS related to an insider threat inquiry.

Overview

The Department of Homeland Security (DHS) Insider Threat Program (ITP) was established pursuant to Executive Order No. 13587[3] and the attendant National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.[4] The ITP may maintain information from any DHS Component, office, program, record, or source, including records from information security, personnel security, and systems security for both internal and external security threats.

The ITP is a Department-wide program to identify threats to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems by collecting and analyzing data about (1) DHS personnel;[5] (2) state, local, tribal, territorial, and private sector personnel who possess security clearances granted by DHS; (3) any person who accesses DHS information technology (IT) systems or DHS information; and (4) any person with access to DHS facilities, information, equipment, networks, or systems. The ITP identifies insider threats through the collection and analysis of data. Once suspected insider threats are identified, the relevant information and analysis is provided by the ITP to the appropriate Component or investigative agency for further investigation and action in accordance with the DHS Insider Threat Operations Center (ITOC) Standard Operating Procedures (SOP), described below.

To the extent this PIA covers the insider threat operations of DHS components, it does so only when those activities fall within the scope of the DHS ITP, which is limited to managing insider threat matters; facilitating insider threat investigations and activities associated with counterintelligence and counterespionage complaints, inquiries, and investigations; identifying threats to DHS resources and information assets; tracking referrals of potential insider threats to internal and external partners; and providing statistical reports and meeting other insider threat reporting requirements. For purposes of the DHS ITP, "insider" is defined as "any person who has or who had authorized access to sensitive or classified national security information, at any DHS facilities, equipment, networks, or systems;" it does not cover other populations that do not have

[3] Exec. Order No. 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 Fed. Reg. 63811 (Oct. 7, 2011), *available at* https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.

[4] Presidential Memorandum — National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (November 21, 2012), *available at* https://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand.

[5] Throughout the document, "personnel" has the meaning of the word "employee" as provided in section l.l(e) of Executive Order No. 12968, Access to Classified Information, August 2, 1995. Specifically, this refers to a person, other than the President and Vice President, employed by, detailed or assigned to DHS, including members of the Armed Forces; an expert or consultant to DHS; an industrial or commercial contractor, licensee, certificate holder, or grantee of DHS, including all subcontractors; a personal services contractor; or any other category of person who acts for or on behalf of DHS as determined by the DHS Chief Security Officer.

access to one of those delineated departmental resources. This PIA does not cover the activities of the United States Coast Guard (USCG) Insider Threat Program, which operates on different classified and unclassified networks under the purview of the Commandant of the USCG. Information concerning USCG personnel may be captured as they are accessing DHS facilities, resources, or systems.

Program Functions, Data, and Structure

The ITP collects data from three main sources when protecting DHS facilities, information, equipment, network, and systems: (1) software that monitors users' activity on DHS computer networks; (2) information supplied by DHS personnel and prospective personnel that is provided to the Department to gain access to DHS facilities, information, equipment, networks, or systems; and (3) tips and leads received by other means, such as email or telephone. The ITOC may receive a tip from any party, including members of the public. Additional sources of data are identified in Section 2.2 below. The ITP collects, uses, disseminates, and retains this data in accordance with the DHS ITP System of Records Notice (SORN).[6]

The DHS ITOC, which serves as the centralized hub for the DHS ITP, collects and maintains data from the three sources identified above. The ITOC is comprised of analysts with extensive training in security and counterintelligence who electronically monitor and analyze the activities of personnel on DHS IT systems and within DHS facilities. The ITOC accomplishes its mission to protect information, networks, and systems by using two types of commercially available proprietary software tools: monitoring software and analytical software.

All persons accessing DHS IT systems or networks are confronted with a banner during the logon process that requires the person to acknowledge the following:

> You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
>
> Unauthorized or improper use or access of this system may result in disciplinary action, as well as civil and criminal penalties.
>
> By using this information system, you understand and consent to the following:
>
> You have no reasonable expectation of privacy when you use this information system; this includes any communications or data transiting or stored on this information system.
>
> At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search and seize any communication or data transiting or stored on this

[6] DHS/ALL-038 Insider Threat Program System of Records, 81 FR 9871 (Feb. 26, 2016).

information system.

The government may disclose or use any communications or data transiting or stored on this information system for any lawful government purpose, including but not limited to law enforcement purposes.[7]

The ITOC uses monitoring software to alert ITOC analysts of anomalous activity by users on DHS IT systems when certain conditions are met. These conditions, which are known as policies, give rise to automated alerts or "triggers," which can be automatically reviewed by analytical software or manually reviewed by ITOC analysts to determine if the anomalous activity is indicative of an insider threat. All of the triggers and policies are approved by the Insider Threat Oversight Group (ITOG) prior to implementation. Triggers identified by the ITP are designed to detect Insider Threats pertaining to espionage, terrorism, unauthorized disclosure of information, and workplace violence. The ITP may use intelligence community reporting or law enforcement information to develop triggers. Additionally, supplemental triggers may be identified and deployed in support of a lawful criminal or administrative investigation when such support is expressly authorized by the ITOG. When triggers are based on specific reports, law enforcement information, or criminal or administrative investigations, the ITP retains a copy of the information serving as the basis for the trigger, as appropriate, to (a) demonstrate the validity of the trigger if the program is audited, (b) understand the basis for the trigger if network activity trips it, and (c) to analyze trends in anomalous behaviors over time.

The ITOG is comprised of cleared representatives from the Office of General Counsel, Intelligence Law Division (OGC/ILD); the Privacy Office (PRIV); and the Office for Civil Rights and Civil Liberties (CRCL). The ITOG reviews the proposed policies referenced above to ensure that: (1) they are consistent with applicable provisions of the Constitution, statutes, executive orders, presidential or other directives, regulations, international or domestic agreements or arrangements, and government-wide or departmental policy; (2) that they do not violate privacy protections relating to the use, collection, retention, and disclosure of personally identifiable information (PII) of any individuals and that any PII revealed as a result of the trigger or contained in Privacy Act systems of records is handled in full compliance with the Fair Information Practice Principles (FIPPs); and (3) they do not violate the civil rights and civil liberties of any individual and that the policy complies with any legal, regulatory, policy, or other requirements relating to the civil rights and civil liberties of individuals. Once approved, the policies are uploaded into the

[7] This is the banner on B and C LAN. The A-LAN banner changes the last two sentences as follows:
At any time, and for any lawful government purpose, the government may, without notice, monitor, intercept, search and seize any communication or data transiting or stored, *originated from or directed to or from* this information system. The government may disclose or use any communications or data transiting or stored, *originated from or directed to or from* this information system for any lawful government purpose.

monitoring tool for deployment.

The ITOC uses the analytical software in a similar manner as the monitoring software described above. Specifically, the ITOC identifies relevant data for analysis (which may include, system and network audit logs, personnel security records and personal information resulting from their background investigations, subsequent vetting, or during the hiring process), other DHS owned information and publicly available information to the DHS ITP "Bulk Data Procedures" located in Appendix A, the ITOC—in coordination with the ITOG and consistent with the ITP governance procedures—works to ingest the data and run automated analysis in order to identify insider threats.

When triggers occur on the monitoring or analytical software, they are analyzed by the ITOC, along with all other information available to the ITOC, in order to help the ITOC determine whether an insider may pose an insider threat. Following a trigger from the monitoring or analytical software, the ITOC may gather additional data, including relevant PII and additional data from monitoring the user's IT systems, to determine whether an insider may be an actual insider threat.

Additional data gathered from targeting the user's IT systems without his or her knowledge is known as "enhanced user activity monitoring" and refers to the technical ability of the monitoring software to gather more information on a particular insider for a particular length of time. Enhanced user activity monitoring requires the formal written approval of the Chief Security Officer (CSO) and concurrence by the ITOG, as set out in the DHS ITP SOP. There is an immutable audit log associated with this activity, which ensures that the ITOC only conducts this activity in accordance with the SOP. The ITOC's collection of this information is consistent with the consent granted by the insiders when they acknowledge the conditions under which usage is granted in the logon banners (provided in full above). Furthermore, the ITOG has the authority to audit the ITOC's logs to ensure that enhanced monitoring is conducted in accordance with the President's National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs and the ITOC SOP.

Due to the sensitive nature of the PII accessed by the ITOC, the ITOC is virtually and physically separated from the enterprise DHS Top Secret//Sensitive Compartmented Information computing environment such that systems administrators (including privileged users), are blocked from accessing the tools, data, and information available to the ITOC. This technical solution serves to ensure the confidentiality and integrity of the sensitive PII and related data maintained by the ITOC. The data is also procedurally separated, being maintained solely in the ITP unless the information meets the threshold for a referral to organizations such as the Office of the Inspector General (OIG), the Office of Intelligence and Analysis (I&A) Counter Intelligence Division (CID), or appropriate component investigative organizations. This referral process insulates the ITOC from sharing the data prior to a formal referral.

In addition to utilizing monitoring and analysis software to identify insider threats, the ITOC also receives reporting (tips and leads) from DHS personnel and members of the public regarding potential insider threats. This reporting is an essential element of the ITOC business process because many indicators of insider threat activity are not captured by the monitoring and analytical software discussed above. The ITOC receives reporting via referrals from other offices within DHS, walk-ins, phone calls, classified and unclassified emails, and a website that is available to all DHS personnel (http://dhsconnect.dhs.gov/Pages/Insider_Threat_Program.aspx).

As mandated by the President's National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, the ITOC aggregates and assesses available information for insider threats by cross-referencing the triggers described above, against other data maintained by the Department and open source information. Foreign travel, reports of foreign contacts, facility access records, and security incident reporting are some examples of data that may be used to conduct analysis. In accordance with the Bulk Data Procedures located in Appendix A, the ITOC ingests various datasets for analysis and correlation in order to identify potential insider threats. The data ingested and analyzed by the ITOC is collected, collated, and subjected to analysis inside the ITOC on a Top Secret//Sensitive Compartmented Information accredited IT system.

By analyzing the data derived from the monitoring software, integrating other DHS data through bulk data transfers from select sources combined with open source information, and applying automated analysis to the data, the ITOC is able to establish a holistic picture of any given insider. Accordingly, to perform the ITOC's Insider Threat Mission, access to this information, including PII, in both manual and automated formats is essential, because the ITOC's core function is to monitor and analyze the activities of insiders in order to assess observed individual behaviors indicative of an insider threat.

In accordance with the Bulk Data Procedures, the ITOC receives annual specialized training from the ITOG regarding the collection, use, dissemination, and retention of information, to include PII. The ITOG provides this specialized training on supplemental policies and procedures prior to an analyst accessing the data, and once per year thereafter. In addition, such personnel consult with the ITOG prior to developing or implementing any automated information system to be maintained by the ITP that is reasonably likely to contain significant amounts of PII.

The ITOC does not directly conduct any investigative or enforcement activities. When certain thresholds are met, as established by the ITOC SOP, the ITOC refers insider threat matters to appropriate entities for further inquiry or investigation. These entities include the OIG, the Office of the Chief Security Officer (OCSO), I&A, Component offices that address internal affairs or security, the Intelligence Community, or other federal agencies with appropriate jurisdiction such as the Federal Bureau of Investigation (FBI). A Component or office receiving an ITOC referral uses its own existing legal authorities to conduct any required administrative or

investigative activity resulting from the ITOC referral. No additional authorities are gained or implied as an extension to the ITOC. The ITOC retains records on matters referred to Components and other offices and records final disposition or resolution of referred insider threat matters.

In addition to these protections, the DHS Privacy Office maintains the authority to conduct a privacy compliance review of the system's operational deployment at any time with reasonable notice to ITP leadership.

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?

DHS is authorized to collect this information pursuant to the following:

1. Executive Order 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information;[8]
2. Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs;[9]
3. DHS Delegation of Authority 08503 (Aug. 10, 2012);
4. DHS Directive 262-05, Information Sharing and Safeguarding (Sept. 4, 2014);
5. DHS Instruction 262-05-01, Insider Threat Program (July 9, 2015);
6. Title 6 U.S.C. §341(a)(6), Under Secretary for Management;
7. DHS Directive 121-01, Office of the Chief Security Officer (Feb. 2014);
8. DHS Delegation Number: 12000, Delegation for Security Operations within DHS (June, 2012); and
9. DHS Directive 11052, Internal Security Program (Oct. 2004).

In addition to the authorities above, the collection of information regarding the eligibility of personnel for security clearances is authorized by:

1. Atomic Energy Act of 1954;[10]

[8] Exec. Order No. 13587 - Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 Fed. Reg. 63811 (Oct. 7, 2011), *available at* https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net.
[9] Presidential Memorandum - National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012), *available at* https://www.whitehouse.gov/the-press-office/2012/11/21/presidential-memorandum-national-insider-threat-policy-and-minimum-stand.
[10] 60 Stat. 755 (Aug. 1, 1946).

2. Title 6 U.S.C. § 341(a)(6), Under Secretary for Management;
3. Title 28 U.S.C. § 535, Investigation of Crimes Involving Government Officers and Employees; Limitations;
4. Title 40 U.S.C. § 1315, Law Enforcement Authority of Secretary of Homeland Security for Protection of Public Property;
5. Title 50 U.S.C. § 3381, Coordination of Counterintelligence Activities;
6. Executive Order 12333 - United States Intelligence Activities (as amended);[11]
7. Executive Order 12829 - National Industrial Security Program;[12]
8. Executive Order 12968 - Access to Classified Information (as amended);[13]
9. Executive Order 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information;[14]
10. Executive Order 13488 - Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, January 16, 2009;[15]
11. Executive Order 13526 - Classified National Security Information;[16]
12. Executive Order 13549 - Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities;[17]
13. By the regulations found at 5 C.F.R. parts 731, 736, and 1400, 32 CFR Part 147;

[11] Exec. Order No. 12333 - United States Intelligence Activities, 46 Fed. Reg. 59941 (Dec. 8, 1981), *available at* http://www.archives.gov/federal-register/codification/executive-order/12333.html.
[12] Exec. Order No. 12829 - National Industrial Security Program, 58 Fed. Reg. 3479 (Jan. 6, 1993), *available at* http://www.archives.gov/federal-register/codification/executive-order/12333.html.
[13] Exec. Order No. 12968 - Access to Classified Information, 60 Fed. Reg. 40245 (August 2, 1995), *available at* http://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf.
[14] Exec. Order No. 13467 - Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, 73 Fed. Reg. 38103 (June 30, 2008), *available at* http://www.gpo.gov/fdsys/pkg/FR-2008-07-02/pdf/08-1409.pdf.
[15] Exec. Order No. 13488 - Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, 74 Fed. Reg. 4111 (Jan. 16, 2009), *available at* http://www.gpo.gov/fdsys/pkg/FR-2009-01-22/pdf/E9-1574.pdf.
[16] Exec. Order No. 13526 - Classified National Security Information, 75 Fed. Reg. 707 (Dec. 29, 2009), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-01-05/pdf/E9-31418.pdf.
[17] Executive Order 13549 - Classified National Security Information Programs for State, Local, Tribal, and Private Sector Entities, 75 Fed. Reg. 51609 (August 18, 2010), *available at* http://www.gpo.gov/fdsys/pkg/FR-2010-08-23/pdf/2010-21016.pdf.

14. Intelligence Community Directive (ICD) 704;[18] and

15. DHS Delegation 12000, Chief Security Officer (June 5, 2012).

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

The DHS/ALL-038 Insider Threat Program SORN[19] covers all records and information used by DHS ITP related to the management and operation of DHS programs to safeguard DHS resources and information assets. The SORN covers both classified and sensitive but unclassified information (often marked by DHS as For Official Use Only (FOUO)).

Data covered by other DHS SORNs is only ingested by the ITOC in accordance with the "Procedures for the Insider Threat Program Concerning Bulk Data Transfers" located in Appendix A and consistent with the provisions of the Privacy Act.

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

A classified system security plan (SSP) has been completed supporting the monitoring and analytical tools utilized by the ITOC. The monitoring and analytical tools received final authority to operate on March 18, 2014.

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

Yes. Records in DHS/ALL-038 Insider Threat System of Records are subject to the National Archives & Records Administration General Records Schedule 5.6: Security Records (July 2017), which mandates that (a) records pertaining to an "insider threat inquiry"[20] are destroyed 25 years after the close of the inquiry; (b) records containing "insider threat information"[21] are destroyed when 25 years old; (c) insider threat user activity monitoring (UAM)

[18] Intelligence Community Directive (ICD) 704 (Oct. 1, 2008), *available at* http://www.dni.gov/files/documents/ICD/ICD_704.pdf.
[19] DHS/ALL-038 Insider Threat Program System of Records 81 FR 9871 (Feb. 26, 2016).
[20] "Insider threat inquiry records" are defined as "records about insider threat program inquiries initiated or triggered due to derogatory information or [the] occurrence of an anomalous incident," including, but not limited to, "initiated and final reports, referrals, and associated data." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 220, 103 (July 2017).
[21] "Insider threat information" is defined as "data collected and maintained by insider threat programs undertaking analytic and risk-based data collection activities to implement insider threat directives and standards," including, for example, the following categories of information: "counterintelligence and security information;" "information assurance information;" "human resources information;" "investigatory and law enforcement information;" and "public information." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 230, 104 (July 2017).

data[22] is destroyed no sooner than 5 years after the inquiry has been opened, but longer retention is authorized if required for business use; and (d) insider threat administrative and operations records[23] are destroyed when 7 years old.

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.

The ITP does not collect information covered by the PRA.

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.

The ITP, specifically the ITOC, requires information from various sources to perform its mission to safeguard DHS resources and information assets. The ITP derives information for analysis from multiple sources within the Department, including network and system audit logs, information assurance, security, and counterintelligence, human resources, law enforcement files, and reports, including from open source information. The list of specific datasets to which the ITOC has access is located in Appendix B, which is classified pursuant to the U.S. Insider Threat Security Classification Guide.

The ITOC uses automated computer monitoring data, IT audit logs, facility physical access control records, security files (to include personnel security file information; records of violations, infractions, and incidents; and security clearance information), counterintelligence information, personnel files containing information about misconduct and adverse actions, law enforcement

[22] "Insider threat user activity monitoring (UAM) data" is defined as "user attributable data collected to monitor user activities on a network to enable insider threat programs and activities to: identify and evaluate anomalous activity involving National Security Systems (NSS); identify and assess misuse (witting or unwitting), or exploitation of NSS by insiders; [and] support authorized inquiries and investigation." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 240, 105 (July 2017).
[23] "Insider threat administrative and operational records" are defined as "records about insider threat program activities" including, for example, "correspondence related to data gathering;" "briefing materials and presentations;" "status reports;" "procedures, operational manuals, and related development records;" "implementation guidance;" "periodic inventory of all information, files, and system owned;" "plans or directives and supporting documentation, such as independent self-assessments, corrective action plans, [and] evaluative reports." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 210, 103 (July 2017).

investigatory data, travel data, financial data, disclosure statements, and open source information to automatically and manually analyze the data for insider threats.

As explained above, the ITOC applies analytic tools to the data collected on DHS networks and to other data sets afforded to the ITOC that are collected via bulk data ingest from other systems of record in accordance with the procedures in Appendix A. The intent of gathering the information is to allow the ITOC to evaluate and assess anomalous activities to identify potential insider threats at DHS.

The ITOC may collect the following types of information:

- Information related to DHS security investigations, including authorized physical, personnel, and communications security investigations, and information systems security analysis and reporting, including:
  - Name(s);
  - Date and place of birth;
  - Social Security number (SSN);
  - Address(s);
  - Personal and official email addresses;
  - Citizenship;
  - Personal and official phone numbers;
  - Driver license numbers,
  - Vehicle identification numbers,
  - License plate numbers;
  - Ethnicity and race;
  - Work history;
  - Educational history;
  - Information on family members, dependents, relatives, and other personal associations;
  - Passport numbers;
  - Gender;
  - Hair and eye color;
  - Biometric data;

- Other physical or distinguishing attributes of a person;
- Medical reports;
- Publicly available social media account information concerning the person;
- Access control pass, credential number, or other identifying number; and
- Photographic images, videotapes, DVDs; and
- Other information provided to DHS to obtain access to DHS facilities or information systems.

- Records relating to the management and operation of DHS physical, personnel and communications security program, including:
  - Completed standard form questionnaires issued by United States Office of Personnel Management (OPM);
  - Background investigative reports and supporting documentation, including criminal background, medical, and financial data;
  - Other information related to a person's eligibility for access to classified information;
  - Criminal history records;
  - Polygraph examination results;
  - Logs of computer activities on all DHS IT systems or any IT systems accessed by DHS personnel with security clearances;
  - Nondisclosure agreements (NDA);
  - Document control registries;
  - Courier authorization requests;
  - Derivative classification unique identifiers;
  - Requests for access to sensitive compartmented information (SCI);
  - Records reflecting personal and official foreign travel;
  - Facility access records;
  - Records of contacts with foreign persons; and
  - Briefing/debriefing statements for special programs, sensitive positions, and other related information and documents required in connection with personnel security clearance determinations.

- Reports of investigations regarding security violations or misconduct, including:
  - Individual statements or affidavits and correspondence;
  - Incident reports;
  - Drug test results;
  - Investigative records of a criminal, civil, or administrative nature;
  - Letters, emails, memoranda, and reports;
  - Exhibits, evidence, statements, and affidavits;
  - Inquiries relating to suspected security violations;
  - Recommended remedial actions for possible security violations; and
  - Personnel files containing information about misconduct and adverse actions.
- Any information related to the management and operation of the DHS insider threat program, including:
  - Documentation pertaining to investigative or analytical efforts by DHS ITP personnel to identify threats to DHS personnel, property, facilities, and information;
  - Records collated to examine information technology events and other information that could reveal potential insider threat activities;
  - Travel records;
  - Intelligence reports and database query results relating to insiders covered by this system;
  - Information obtained from the Intelligence Community (IC) or from other agencies or organizations about persons known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to an insider threat, including but not limited to espionage or unauthorized disclosures of sensitive or classified national security information;
  - Information provided by record subjects and individual members of the public; and
  - Information provided by individuals who report known or suspected insider threats.

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

Sources of information are the records created whenever a person accesses/uses any DHS facilities, information, equipment, networks, or systems; and any relevant records obtained through bulk sharing as detailed in the Insider Threat Operations Center Analytic Activities SOP Appendix C: Procedures for the Insider Threat Program Concerning Bulk Data Transfers. Consistent with language contained in 2.1 above, the ITOC gathers information from multiple sources on persons who have access to any DHS facilities, information, equipment, networks, or systems.

Records are obtained from Department officials, employees, contractors, and other individuals who are associated with or represent DHS; officials from other foreign, federal, tribal, state, and local government organizations; non-government, commercial data aggregators, public, and private agencies and organizations; relevant DHS records, databases, and files, including personnel security files, facility access records, security incidents or violation files, network security records, investigatory records, visitor records, travel records, foreign visitor or contact reports, and financial disclosure reports; media, including social media, periodicals, newspapers, and broadcast transcripts; intelligence source documents; and complainants, informants, suspects, and witnesses.

The ITOC collects information maintained by the Office of the Chief Security Officer, as well as other offices in the Department, that is collected with consent from personnel to whom the record pertains both during onboarding and while employed by their employer or DHS. This includes state, local, tribal, territorial, and private sector personnel who have access to any DHS facilities, information, equipment, networks, or systems.

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

Yes. In order to verify information and develop leads from the monitoring and analytic software discussed above, the ITOC gathers information from commercially available data sources and publicly available electronic information to clarify or resolve suspected insider threats.

2.4 Discuss how accuracy of the data is ensured.

ITOC analysts use a variety of data sources available through the source systems to verify and corroborate the available information to the greatest extent possible. Ensuring the accuracy of the data depends on the system(s) performing the original collection.

The accuracy of DHS-owned data, other federal agency data, as well as data provided by commercial data aggregators, is dependent on the original source. ITOC analysts are required by

policy to alert data owners if records in an underlying system of record are identified as inaccurate. The ITOC's records then reflect the corrected information. Additionally, as the source systems for other federal agency data or commercial data aggregators correct information, queries of those systems reflect the corrected information.

ITOC analysts are required to vet data in accordance with standard operating procedures and training manuals to ensure that the data used is accurate. ITOC analyst-provided information is stored in a collaborative workspace where other analysts can review and challenge it. Insider threat referrals are subject to peer review, supervisor review, and OGC/ILD review to ensure accuracy before the ITOC makes an insider threat referral. As with other leads, information obtained through searches of publicly available electronic media is analyzed against other sources for corroboration.[24]

If erroneous information is included in an insider threat referral, a revised referral is sent to correct the information or note the questionable fact or content, and the incorrect referral is removed from the ITOC's repository. For any referrals that were externally disseminated and need recall or correction, a recall message or revised referral is disseminated to the recipients of the original product(s) with appropriate instructions.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

In addition to the risks accumulated by the underlying systems that the ITOC accesses, the following potential risks related to the ITOC's collection of data have been identified:

Privacy Risk: The ITP Bulk Data Transfers include the collection or dissemination of large quantities of intelligence or information, a significant portion of which is not reasonably likely to have any ultimate investigative value to the ITOC, but which is provided to the ITOC to permit identification of information with investigative value contained within. Therefore, there is a heightened risk of over-collection.

Mitigation: This risk is partially mitigated as follows: all ITP Bulk Data Transfers are subject to the Bulk Data Procedures located in Appendix A. The procedures require all transfers to be subject to written terms and conditions that are coordinated with and approved by PRIV, CRCL, and OGC. The written terms and conditions require that any information acquired by the ITP through bulk data transfer be used only in support of an authorized ITP mission, that the ITOC

[24] Publicly available electronic media is any electronic social media information that has been published or broadcasted for public consumption, is available on the request to the public, is accessible on-line to the public, is available to the public by subscription or purchase, or is otherwise lawfully accessible to the public. For more information, see Security Executive Agent Directive 5, *Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications*, available at https://www.dni.gov/files/NCSC/documents/Regulations/SEAD_5.pdf.

identify and mark (or "tag") PII concerning U.S. Persons and any other Special Protected Classes within the data ingested in bulk, and that the data only be temporarily retained and in accordance with the written terms and conditions. These requirements, along with the others outlined in Appendix A, are designed to ensure that the ITOC can conduct its mission while protecting the privacy rights, and the civil rights and civil liberties of all individuals.

Privacy Risk: The behavioral indicators used to create triggers for additional analysis—which are identified by the ITOC through analysis of historical trends and specific conduct and subsequently approved by the ITOG— are not inherently criminal.

Mitigation: The indicators that lead to additional analysis are simply viewed as an initial factor and must be corroborated by multiple factors to move through the examination process. The ITP tool suite is able to compare anomalous behaviors amongst cohorts of users to weigh the relative significance of any given trigger. The process is well defined in the ITOC SOP, which explains the levels of inquiry and the thresholds to progress through the inquiry process. The analysis done on the basis of a tip or an anomaly in behavior is considered a preliminary inquiry and the ITOC analyst has a defined set of systems that can be accessed to assess the implications of the anomaly. OGC/ILD must be notified when the ITOC initiates a preliminary inquiry. Within five days the preliminary inquiry must have identified additional verified concerns to OGC/ILD or be closed.

Privacy Risk: More information than is necessary will be analyzed in order to determine if an actual insider threat exists.

Mitigation: When the ITOC is alerted by automated triggers, workforce reports, or incoming tips and leads to a potential insider threat, the ITOC conducts research following a standardized protocol of checks to review information that may or may not corroborate the initial insider threat concern. If the information examined by the ITOC does not corroborate the insider threat concern, it could be argued that the information viewed was unnecessary. However, the ITP can neither corroborate nor mitigate an insider threat concern unless it accesses the relevant information sets. The ITOC only queries additional data when necessary and appropriate to resolve an insider threat concern. Furthermore, all ITOC activities are overseen by the DHS Chief Security Officer, the ITP Manager, the ITOG (which includes OGC, CRCL, and PRIV representatives), and the ITOC Director to ensure compliance with applicable laws, regulations, and policies.

Privacy Risk: Because the ITOC draws upon data aggregators from DHS, other federal agencies, and commercial entities to obtain data instead of collecting directly from individuals, there is a risk that ITOC data will become outdated and inaccurate.

Mitigation: The ITOC routinely refreshes data from its various source systems, consistent with the written terms and conditions required by the Procedures for the Insider Threat Program Concerning Bulk Data Transfer (Appendix A) so that the ITOC systems accurately reflect any

changes to the records contained in the underlying source systems and the addition or deletion of those records. When an ITOC analyst accesses a record, the record is also retrieved from the underlying source system to ensure that only the most current data is available to the ITOC analysts. Additionally, when an ITOC analyst conducts a query, any changes, additions, or deletions of records from commercial data aggregators are reflected in that query.

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.

The collection of this information allows ITOC analysts to determine if there is an indication that a person might constitute an insider threat and if so, generate a referral that would better inform the receiving component or office about the nature of the insider threat. In order to determine whether a particular person is an insider threat, ITOC analysts may use information available to the ITOC from a variety of sources to make possible a more complete view of the person. The analyst then analyzes and interprets the data using the available visualization and collaboration tools.

ITOC analysts use the aggregated data, as well as the monitoring and analytical software tools, to identify actions or relationships that may pose insider threats. When an ITOC analyst conducts a search, the ITOC system performs the query on the index, as well as across multiple other federal and commercial systems. Indexed data facilitates efficient searching of large databases for terms that occur in field limited or free-text data. Only ITOC analysts authorized to access the data can perform these searches. In allowing ITOC analysts to perform a single query across multiple systems and databases, the ITOC reduces the time spent searching each individual system and reduces the load that would be placed on those systems through repeated queries. ITOC analyst-provided information and data obtained from commercial sources is used to complement, clarify, or provide context to data from internal DHS sources.

ITOC analysts use the analytical tools to create insider threat referrals in accordance with the ITOC SOP. ITOC analysts maintain control of the raw data in the analytical tool. ITOC analysts archive this data upon completion of an insider threat referral in accordance with the ITOC SOP. If an ITOC analyst finds actionable terrorism-related, law enforcement, security, or counterintelligence information after conducting a search and performing analysis on the raw data, they may use relevant information to produce a referral.

ITOC referrals are sent to the appropriate DHS Components or federal agencies for subsequent action based upon the insider threat issue identified. Recipients can include the DHS OIG, OCSO, I&A, Component offices that address internal affairs or security, members of the U.S. Intelligence Community, or other federal agencies with appropriate jurisdiction over the

insider threat issue identified.

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.

Yes. ITP monitoring and analysis software may use predictive analysis or look for patterns of behavior. When this is done, this information is solely used as an indicator that requires additional review of the information and the context. This program is reportable under the Data Mining Act.

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

Yes. Currently, the ITOC is comprised of DHS Office of the Chief Security Officer employees, contractor representatives who support the monitoring and analytic software, and counterintelligence employees on detail from the I&A. Other DHS Components or federal agencies do not have access to ITOC systems except for component detailees assigned to the ITOC on a full-time basis as analysts and component POCs, who are subject to the same oversight as all ITOC members. Also, information from the ITOC is provided to DHS Components or other federal agencies when the ITOC creates a referral in accordance with the ITOC SOP.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: When information is gathered to assess whether an insider threat exists, there is a risk the information will reveal other information that could result in an adverse action being taken against an individual outside the scope of the insider threat program. For example, an analysis of information could result in identifying that an individual has committed a criminal act or misconduct, even if the same evidence to support that decision does not indicate an insider threat.

Mitigation: Although the ITOC monitoring focuses specifically on insider threat, derogatory information relevant for other purposes must be reported. This privacy risk is mitigated by due process procedures in place when adverse action is taken, both within and outside of DHS. Examples of these processes include filing an appeal with the DHS Security Appeals Board for security clearance matters; the DHS grievance process for human resource actions; and filing a complaint with the OIG, Office of Special Counsel, or the Merit Systems Protection Board for whistleblower matters.

Privacy Risk: There is a risk that members of the ITOC will review data that is not relevant to analysis of insider threats.

Mitigation: The ITOC SOP guides the analyst's review of data needed to resolve instances

that are reasonably indicative of an insider threat. The periodic review of immutable audit logs by the ITOG to ensure that the ITOC analysts are complying with the ITOC SOP also helps mitigate this risk.

Privacy Risk: ITOC analysts with authorized access could use their access for unapproved or inappropriate purposes, such as performing searches on themselves, friends, relatives, or neighbors.

Mitigation: The monitoring and analytic software records the activities of all users to facilitate auditing. Audit trails are created throughout the analytic process and are reviewed if a problem or concern arises regarding the use or misuse of the information. These audit logs are reviewed periodically by cleared representatives from the ITOG and any inappropriate use is referred to the appropriate internal investigators (such as the OIG or others as required) for handling. The detection of inappropriate use also results in the suspension of the analyst's access to ITOC systems until the use can be investigated. The ITOC's auditing capabilities are discussed in greater depth later in this document. This auditing capability ensures that mishandled information is brought to the attention of the ITOC so that corrective action might be taken. The presence of an auditing capability may also serve as a deterrent to willful misconduct by ITOC personnel.

Audit trails are created throughout the analytic process, and are reviewed if a problem or concern arises regarding the use or misuse of the information. When ITOC personnel log in, they must acknowledge and consent to monitoring in order to access the system. Generally, U.S. Government employees and contractors are deemed to have a decreased expectation of privacy in their use of Government equipment, especially when they have consented to monitoring. ITOC analysts are also required to sign specific NDAs (DHS Form 11058), which further reiterates analysts assigned to the ITOC have no reasonable expectation of privacy when using ITOC systems; activity in the ITOC is subject to monitoring and review at all times.

Privacy Risk: Because the ITOC compiles data from multiple systems, users will access information from several systems that were not previously accessible in one system. Some information compiled is not necessarily indicative of illegal activity and could be taken out of context.

Mitigation: Information identified and accessed through the ITOC for the purpose of identifying insider threats must bear a rational relationship to the scope of the analysis contained in the referral. The clearance process for issuing an insider threat referral involves supervisory and legal review to ensure that the analysis and conclusions of the referral are germane to the purpose for which the referral was intended.

Privacy Risk: The ITP SOP permits analysts to conduct their own analysis and incorporate data from commercial data aggregators and publicly available sources rather than using only

directly collected information. Therefore, there is a risk that an ITOC analyst, commercial data aggregator, or public source could provide incorrect or biased information (in the case of an analyst, either accidently or purposefully).

Mitigation: The ITOC requires that all ITOC analyst-provided information be fully attributable to the analyst who provided it. The auditing, peer review, and legal oversight functions further serve to mitigate this risk. If an ITOC analyst provides incorrect or biased information, the information can be corrected and the ITOC analyst can be disciplined, as warranted.

Data from commercial data aggregators and publicly available sources is vetted by ITOC analysts for accuracy by cross-checking the information against multiple sources. Information in intelligence products from commercial data aggregators and publicly available sources is checked for accuracy using the same review process as other information available to the ITOC.

Privacy Risk: There is a risk that data collected for the ITP mission will be used for a different purpose without notice to the data subject.

Mitigation: This risk is mitigated because the ITOC accesses information from systems that share purposes compatible with the DHS ITP mission. Additionally, much of the information the ITOC collects on federal personnel come from Standard Forms (SF) or other Government forms that contain Privacy Act statements or notices explaining their use. Routine audits of system access and use serve to ensure that ITOC analysts employ information consistent with the purposes for which it was collected. The ITOC and the ITOG ensure that the system architecture does not create access or linkages to other systems that are incompatible with the insider threat mission of the ITOC.

In addition to these protections, the DHS Privacy Office maintains the authority to conduct a privacy compliance review of the system's operational deployment at any time with reasonable notice to ITP leadership.

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.

For data collected by the ITP from DHS IT monitoring, warning banners and user agreements for access to any DHS IT networks notify personnel that they have no reasonable expectation of privacy on DHS IT systems and that their activities are subject to monitoring at all times for all lawful

purposes, which includes monitoring for insider threats. DHS Management Directives 4600.1 "Personal use of Government Office Equipment" and 4900 "Individual Use and Operation of DHS Information Systems/Computers" also informs all personnel that that they have no reasonable expectation of privacy on DHS IT systems and that their activities are subject to monitoring at all times for all lawful purposes.

Outside the computer monitoring discussed above and acceptance or reports, tips, and leads, the ITP does not collect any information directly from the general public and therefore, does not have an opportunity to provide notice of such collection. Notice of collection by the underlying government systems performing the original collection is described in the individual PIAs and SORNs for those systems. Reporting to the ITP is done voluntarily by walk-in, phone, email, or through the DHS Connect Insider Threat Program site. Notice is given to individuals that reporting is not anonymous on the site. Commercial data aggregators collect information from publicly available and proprietary records, and therefore do not provide notice to the individual prior to collection.

This PIA itself supplements the notice provided to personnel about oversight of their activities, including those activities that are conducted for insider threat purposes. Finally, all personnel are required to take annual ITP awareness training that further alerts the workforce to ITOC monitoring activities.

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

All personnel must sign user agreements and consent to monitoring prior to logging on to any DHS IT system. All individuals with access to DHS IT systems are subject to IT system monitoring. Individuals who do not consent to monitoring on IT systems are not permitted to access the systems. The ITP does not collect any other information directly from individuals besides the information collected from the monitoring software. As such, once the individual consents to monitoring, the individual does not have further opportunity to decline to provide information, consent to uses, or opt out of the information collected and used by the monitoring and analysis software.

Additionally, the Government systems from which the ITOC draws information include law enforcement, security, and intelligence systems that collect information individuals are required to provide by statutory mandate, or are collected under a law enforcement or intelligence authority. As such, individuals do not have an opportunity to decline to provide the required information, opt out, or to consent to uses. Further, the ITP does not have the ability to provide individuals with the opportunity to consent to use or decline to provide information to commercial sources because it does not control those systems and cannot provide notice other than through this document.

4.3 Privacy Impact Analysis: Related to Notice

Each of the various systems that perform the original collection, and from which the ITOC draws information, are subject to specific notice requirements and mechanisms for such notification. The ITOC further provides notice via the annual insider threat awareness training that all personnel are required to take. The ITP SORN and this PIA provide additional notice.

Privacy Risk: The ITOC does not always collect information directly from individuals who are being monitored, so individuals may not have notice that their information is used by the ITP.

Mitigation: This risk is partially mitigated. The ITP is covered by a SORN (DHS/ALL-038 Insider Threat Program System of Records) and is publishing this PIA to inform individuals what information is contained within the ITOC and how it is used.

Privacy Risk: Non-DHS users of DHS networks will be unaware that their information and actions are included in the ITP.

Mitigation: This risk is partially mitigated by the ITP SORN and this PIA which provide general notice to non-DHS users that their information may be included in the ITP. Further, individuals who email an official DHS email address should be aware that the content of the email sent to the Department is subject to departmental procedures.

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.

The retention period for the information collected by the ITOC varies depending on the type of data. DHS-owned data is retained in accordance with the SORN for the underlying system from which the data is obtained, as well as the written terms and conditions required by the ITOC's Bulk Data Transfer Procedures. Once an underlying source system deletes or changes the data, the ITOC deletes or changes its data during its next refresh from that system.

Records in Department of Homeland Security/ALL-038 Insider Threat System of Records are subject to the National Archives & Records Administration General Records Schedule 5.6: Security Records (July 2017), which mandates that (a) records pertaining to an "insider threat inquiry"[25] are destroyed 25 years after the close of the inquiry; (b) records containing "insider

[25] "Insider threat inquiry records" are defined as "records about insider threat program inquiries initiated or triggered due to derogatory information or [the] occurrence of an anomalous incident," including, but not limited to, "initiated and final reports, referrals, and associated data." National Archives & Records Administration, General Records

threat information"[26] are destroyed when 25 years old; (c) insider threat user activity monitoring (UAM) data[27] is destroyed no sooner than 5 years after the inquiry has been opened, but longer retention is authorized if required for business use; and (d) insider threat administrative and operations records[28] are destroyed when 7 years old.

5.2 Privacy Impact Analysis: Related to Retention

The ITOC's analytic use of the information gathered by existing systems coupled with its retention policies results in the following risks:

Privacy Risk: The ITP may retain information regarding persons who are suspected of insider threat activity without resolving whether the referral was upheld or vacated by the investigative Component or agency.

Mitigation: When the ITOC makes a referral to an investigative agency to confirm whether an individual is an insider threat, the ITOC requires as a condition of the referral that the receiving Component or agency notify the ITOC of the disposition of the matter referred within 60 days. If the receiving Component or agency does not resolve the referred matter within 60 days, the ITOC requires the receiving entity to provide written updates every 60 days until the matter is resolved. This ensures that the ITOC does not retain information regarding persons who are suspected of being insider threats without obtaining resolution on the underlying matter that was referred to a Component or agency for investigation in a timely manner.

Privacy Risk: Because the ITP accesses and indexes information from other systems, it is possible that incorrect information could be indexed by the ITOC and then corrected in the

Schedule 5.6: Security Records, Item 220, 103 (July 2017).

[26] "Insider threat information" is defined as "data collected and maintained by insider threat programs undertaking analytic and risk-based data collection activities to implement insider threat directives and standards," including, for example, the following categories of information: "counterintelligence and security information;" "information assurance information;" "human resources information;" "investigatory and law enforcement information;" and "public information." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 230, 104 (July 2017).

[27] "Insider threat user activity monitoring (UAM) data" is defined as "user attributable data collected to monitor user activities on a network to enable insider threat programs and activities to: identify and evaluate anomalous activity involving National Security Systems (NSS); identify and assess misuse (witting or unwitting), or exploitation of NSS by insiders; [and] support authorized inquiries and investigation." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 240, 105 (July 2017).

[28] "Insider threat administrative and operational records" are defined as "records about insider threat program activities" including, for example, "correspondence related to data gathering;" "briefing materials and presentations;" "status reports;" "procedures, operational manuals, and related development records;" "implementation guidance;" "periodic inventory of all information, files, and system owned;" "plans or directives and supporting documentation, such as independent self-assessments, corrective action plans, [and] evaluative reports." National Archives & Records Administration, General Records Schedule 5.6: Security Records, Item 210, 103 (July 2017).

underlying system. Consequently, a search by an ITOC analyst could return the outdated information.

Mitigation: The ITOC periodically refreshes the indices built from data residing in underlying systems to ensure that only the most current versions are available to users. Further, when a user accesses individual records matching a search (rather than simply the list of results), the records are retrieved directly from the underlying source system prior to making an insider threat referral. This ensures that users see the most up-to-date information.

Privacy Risk: Many insider threat referrals are based on or contain time-sensitive information. The referrals lose accuracy or relevance after a finite period, and there is a risk that resulting agency actions involving the potential to affect encountered persons will be handled inappropriately because the information is no longer accurate or relevant.

Mitigation: The ITOC SOP sets forth internal timelines for generating referrals after information meeting the requisite threshold is identified in order to ensure that referrals are promptly sent for action. Additionally, ITOC analysts are required to update insider threat referrals if they discover the information previously provided was inaccurate or incorrect.[29]

Privacy Risk: The ITOC may retain more information than is necessary when the data fails to indicate a potential insider threat.

Mitigation: The risk is mitigated because pursuant to the ITOC SOP, when insider threat concerns are reported to the ITOC that do not reach the threshold of an insider threat inquiry, the information is permanently anonymized or deleted within 180 days if the information has not been associated with an identified cleared individual and has not been sent out as a referral.

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.

Yes. When an insider threat is identified and it is determined classified information was disclosed in an unauthorized manner to a foreign power or an agent of a foreign power, DHS is required by 50 U.S.C. § 3381(e) to notify the Federal Bureau of Investigation (FBI) and provide access to any DHS records needed for investigative purposes. If other misconduct that raises law

[29] *See* the ITP "Bulk Data Procedures" in Appendix A.

enforcement or other national security concerns is uncovered by the ITOC, the misconduct is referred to the appropriate investigative agency at the federal, state, or local level. All information shared outside of DHS by the ITOC is placed on a formal letterhead memorandum, as well as reviewed and cleared for dissemination in accordance with the ITOC SOP. Any information shared with other federal agencies, state, and local authorities, and the private sector is shared in a manner consistent with the relevant routine use identified in the ITP SORN.

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

The sharing of PII outside of the Department is compatible with the original collections listed in the SORNs of the source systems. Generally, information is shared for law enforcement, intelligence, or national security purposes and with contractors working for the Federal Government to accomplish agency functions related to the system of records, i.e., to counter potential and actual insider threats.

6.3 Does the project place limitations on re-dissemination?

Recipients of information from the ITP are provided the information consistent with their authorities to investigate or take action on the referral. These recipients maintain the information consistent with their authorities and report the resolution back to DHS ITP. DHS has negotiated Memoranda of Agreement (MOA) with all external organizations to which the ITP would refer, which requires those organizations to acquire consent from the ITOC prior to re-dissemination. As a condition of accessing ITOC data, Components are required to get consent from the ITOC for re-dissemination. Only individuals with a need-to-know are able to gain access to ITOC data or ITOC referrals. Generally, non-DHS individuals do not have access to the ITOC monitoring or analytical software systems within the ITOC.

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

The ITP uses the existing processes and procedures within DHS for recording disclosures of information as appropriate to the situation causing the disclosure, and it does not establish or maintain an additional record of the disclosures within the ITOC's systems. Policies and procedures in use include: DHS Directive 047-01 Privacy Policy and Compliance, DHS Instruction 047-01-001 Privacy Policy and Compliance, DHS Form 191 Accounting for Disclosure, DHS Form 11000-8 Disclosure Record, DHS Form 11000-10 Document Record of Transmittal, and DHS Form 11000-10 Record of Security Violation.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: Authorized users are exposed to PII as a routine part of their official duties. These users may make inappropriate disclosure of this information, either intentionally or unintentionally.

Mitigation: All ITOC analysts are required to complete annual specialized privacy training, including the appropriate and inappropriate uses and disclosures of the information they receive as part of their official duties. The analysts' use of the system and access to data is monitored and audited by the ITOG. Should a user inappropriately disclose this information, they are subject to loss of access and disciplinary action up to and including termination. Additionally, all ITOC analysts are required to sign DHS Form 11058, which contains specific provisions regarding the non-disclosure of ITOC information without the appropriate permissions and approvals.

Privacy Risk: ITOC referrals containing incorrect information may be disseminated.

Mitigation: This risk is mitigated through policies describing the correction and re-dissemination process. All referrals that leave the ITOC are marked with their classification and are subject to re-dissemination restrictions.

Privacy Risk: There is a privacy risk that more information than necessary will be shared externally.

Mitigation: This risk is mitigated because that prior to any external disclosure of information, the ITOC Director and DHS OGC review all referrals in order to minimize the amount of information shared to the least amount necessary in order for the recipient to perform their official responsibilities. The ITOG monitors compliance with this requirement through quarterly audits as required by the ITOC SOP.

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?

Because the ITOC systems contain sensitive information related to intelligence, counterterrorism, and homeland security, as well as law enforcement programs, activities, and investigations, DHS has exempted the ITP system and the records therein from the access and amendment provisions of the Privacy Act of 1974, pursuant to 5 U.S.C. §§ 552a(j)(2), (k)(1), (k)(2), and (k)(5).

Regarding specific index data and source data, as described under "Categories of Records" in the published SORN, to the extent that a record is exempted in a source system, the exemption continues to apply. To the extent there is no exemption for giving access to a record under the source system, DHS will provide access to the information maintained in the ITP system.

Notwithstanding the applicable exemptions, DHS reviews all such requests for information on a case-by-case basis. When such a request is made, and access would not appear to interfere with or adversely affect the national or homeland security of the United States or activities related to any investigatory material contained within this system, the applicable exemption may be waived at the discretion of DHS, and in accordance with procedures and points of contact published in the applicable SORN. Individuals seeking notification of and access to any record contained in this system of records, may submit a Freedom of Information Act (FOIA) or Privacy Act request in writing to:

Chief Privacy Officer/Chief Freedom of Information Act Officer
Department of Homeland Security
245 Murray Drive, S.W.
STOP-0655
Washington, D.C. 20528

FOIA requests must be in writing and include the requestor's daytime phone number, email address, and as much information as possible of the subject matter to expedite the search process. Specific FOIA contact information can be found at http://www.dhs.gov/foia under *contacts*.

Although DHS has exempted this system from the access and amendment provisions of the Privacy Act, individuals may make a request to view their records. When seeking records about oneself from this system of records (or any other DHS system of records), the request must conform to the Privacy Act regulations set forth in 6 CFR Part 5. An individual must first verify his or her identity, meaning that he or she must provide full name, current address, and date and place of birth. The request must include a notarized signature or be submitted under 28 U.S.C. § 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. Although no specific form is required, forms for this purpose may be obtained from the Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition, the following should be provided:

- An explanation of why the individual believes the Department would have information on him or her;
- Details outlining when he or she believes the records would have been created; and
- If the request is seeking records pertaining to another living individual, it must include a statement from that individual certifying his/her agreement for access to his/her records.

Without this bulleted information, DHS may not be able to conduct an effective search for responsive documentation, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

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

The data accessed by the ITP from source systems may be corrected by means of the processes described in the PIAs for those systems. Because the ITP draws upon other source systems for its data, any changes to source system records (including the addition or deletion of source system records), is reflected in corresponding amendments to the ITP index, as the index is periodically updated.

ITOC analysts are responsible for the integrity and confidentially of the data they provide. Should erroneous information be entered, the analyst is required to correct his or her entry immediately upon determining it is incorrect. This requirement applies to any data to which an analyst has access, not just data provided by the analyst.

At times, erroneous information may be published in an ITOC referral product. When incorrect information is discovered, a revised referral is provided to correct the information or note the questionable fact or content. The incorrect referral is then removed from the ITOC's system. For any referrals that were externally disseminated, and therefore require recall or correction, recall messages or revised referrals are disseminated to the recipients of the original referral(s), with appropriate instructions.

As noted in 7.1 above, requests from the public for information from the ITP are reviewed on a case-by-case basis.

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

Individuals are notified of the procedures for correcting their information through the SORNs describing each of the underlying systems from which the ITP accesses information, as well as the ITP SORN and this PIA.

7.4 Privacy Impact Analysis: Related to Redress

Given the sensitive nature of the ITP, a robust program to permit access, review, and correction of raw information and referrals cannot be provided. This lack of direct access and a formal redress mechanism poses a risk to individual privacy; however, it is pragmatic given the heightened sensitivity of and potential harm to Government activities supported by the ITP. Although individuals do not have a formal mechanism for access or redress, DHS has internal

mechanisms to correct inaccuracies and protect against abuse through the information system security protections and controls established within the ITP system.

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?

The ITP system implements extensive auditing through the various applications that compose the system. Although the specifics of the system and applications are classified, the system logs every action by ITOC analysts. The ITOC's audit logs are immutable and they are subject to quarterly and unannounced reviews by the ITOG. ITOC analysts are not able to access the audit logs. Audit logs are maintained for 25 years. On a retroactive basis, should an incident occur, logs can be reviewed post-incident. The ITOG, along with management, can determine who accessed what information to a certain level of granularity.

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

All ITOC analysts are required to complete specialized annual training in privacy awareness provided by the ITOG. The specialized training is provided by the ITOG on supplemental policies and procedures prior to access to data, and once per year thereafter. In addition, ITOC personnel consult with the ITOG prior to developing or implementing any automated information system to be maintained by the ITP that is reasonably likely to contain significant amounts of PII concerning U.S. Persons. This training is completed in addition to the annual privacy training that all DHS personnel receive and the open source training, which is completed by all ITOC analysts. ITOC analysts who do not complete the required specialized annual training lose access to all computer systems in the ITOC, which are integral to their duties.

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

Only authorized ITOC personnel and analysts who require access to the functionality and data in the ITP as a part of the performance of their official duties and who have appropriate clearances or permissions have access to data. The number of ITOC personnel and analysts is limited in order to prevent widespread access to the sensitive information available to the ITOC. All ITOC personnel and analysts are required to hold and maintain TOP SECRET//SENSITIVE COMPARTMENTED INFORMATION access. Everyone in the ITOC is required to sign a NDA

(DHS Form 11058) specific to the ITOC prior to accessing any ITP data. Any personnel not employed by the DHS Office of the Chief Security Officer are required to be detailed (as opposed to assigned) to the Office of the Chief Security Officer prior to assignment within the ITOC. ITOC operations are conducted in a restricted access Sensitive Compartmented Information Facility in order to maximize the security of the location and effectively monitor the activities of ITOC personnel. If issues are raised concerning ITOC compliance with approved policies and procedures, the issues are immediately reviewed by the ITOG. The ITOG may conduct system audits or policy/procedure reviews and recommend remedial actions to the Senior Insider Threat Official.

DHS maintains ITP access records showing which ITOC analysts have accessed the system, which functions they have used, and which data they have accessed. ITP management revokes a user's access when no longer needed or permitted. No personnel outside of the ITOC are given access to the data until such time a formal referral is provided in accordance with the SOP.

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?

Information sharing agreements, MOUs, new uses of the information, and new access to ITP data by organizations both within DHS and external are reviewed and approved by the ITOG, as required by the DHS ITP Instruction and the ITOC SOP.

8.5 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk: As the ITOC provides access to and retains a wealth of information, it may become a target for unauthorized users (e.g., hackers).

Mitigation: The ITOC employs both system-level security and application-level security, including role-based access control (RBAC) and has undergone a Certification and Accreditation (C&A) process. Additional mitigation steps have been taken virtually and physically separate all ITOC data from the DHS C-LAN, which is the DHS enterprise TOP SECRET//SENSITIVE COMPARTMENTED INFORMATION network. This separation ensures that ITOC data is only stored on a secure, accredited network, which is inaccessible by all other users of the DHS C-LAN.

Further, the ITOC conducts routine audits and system checks to ensure the relevance of controls and markings and to protect the information over time.

Responsible Officials

Richard D. McComb
Senior Insider Threat Official
Chief Security Officer
Department of Homeland Security

David J. Glawe
Under Secretary for Intelligence and Analysis
Department of Homeland Security
Undersecretary for Management

Approval Signature

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

_____

Philip S. Kaplan
Chief Privacy Officer
Department of Homeland Security