Privacy Impact Assessment Update
for the

Insider Threat Program

DHS/ALL/PIA-052(b)

June 16, 2020

Contact Point
Sean Thrash
Insider Threat Program Manager
Office of the Chief Security Officer
202-447-4200

Richard D. McComb
Senior Insider Threat Official
Chief Security Officer

Reviewing Official
Dena Kozanas
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The U.S. Department of Homeland Security (DHS or Department) Insider Threat Program (ITP) was established as a DHS-wide effort to manage insider threat matters. The ITP detects, prevents, and mitigates threats posed to the Department by individuals who have or had authorized access to DHS facilities, information, equipment, networks, or systems while protecting their privacy, civil rights, and civil liberties. DHS is updating this Privacy Impact Assessment (PIA) to account for a new affected population and new types of information the ITP is now authorized to collect and maintain.[1] Originally, the ITP focused on the detection, prevention, and mitigation of unauthorized disclosure of classified information by DHS personnel with active security clearances. The Secretary's approval expands the scope of the ITP to its current breadth: threats posed to the Department by all individuals who have or had access to the Department's facilities, information, equipment, networks, or systems. Unauthorized disclosure of classified information is merely one way in which this threat might manifest. Therefore, the expanded scope increases the population covered by the program to include all those with past or current access to DHS facilities, information, equipment, networks, or systems, regardless of security clearance.

Overview

Executive Order 13587, "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs require the head of each department or agency that operates or accesses classified computer networks to implement an insider threat detection and prevention program to safeguard classified national security information.

The reforms mandated by EO 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs are limited to protecting classified information from unauthorized disclosure. Accordingly, the purpose of the original DHS ITP established pursuant to EO 13587 was scoped to prevent the unauthorized disclosure of classified national security information.

Subsequent to standing up the DHS ITP, the threats the Department faces extend beyond threats of unauthorized disclosure of classified information by DHS-cleared employees. Threats faced include those posed by insiders with and without security clearances engaging in activities that have no nexus to unauthorized disclosure of classified information.

The memorandum *Expanding the Scope of the Department of Homeland Security Insider Threat Program*, approved by Secretary Johnson on January 3, 2017, expanded the scope of the

[1] *See* Expanding the Scope of the Department of Homeland Security Insider Threat Program (Dec. 2016), *available at* https://www.dhs.gov/sites/default/files/publications/s1_signed_taylor_memo_expanding_insider_threat.pdf.

DHS ITP to include the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems. Insiders would include any person who has or who had authorized access to any DHS facilities, information, equipment, networks, or systems.

This PIA still does not cover the activities of the United States Coast Guard Insider Threat Program, which operates on different classified and unclassified networks under the purview of the Commandant of the Coast Guard. Information concerning Coast Guard personnel may be captured, however, when they access DHS facilities, resources, or systems.

Reason for the PIA Update

DHS is updating this PIA to account for the new affected population and new types of information the program is now authorized to collect and maintain pursuant to the memorandum, referenced above. Originally, the ITP focused on the detection, prevention, and mitigation of unauthorized disclosure of classified information by DHS personnel with active security clearances. The memorandum expands the scope of the ITP to its current breadth: threats posed to the Department by all individuals who have or had access to the Department's facilities, information, equipment, networks, or systems. Unauthorized disclosure of classified information is merely one way in which this threat might manifest. Therefore, the expanded scope increases the population covered by the program to include *all* those with past or current access to DHS facilities, information, equipment, networks, or systems.

The new definitions of "Insider Threat" and "Insider" expands upon the definitions found in EO 13587 and the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.[2] The DHS updated definition of an "Insider," as defined in DHS Instruction 262-05-002, is any person who has or who had authorized access to any DHS facility, information, equipment, network, or system. An "Insider Threat" is now defined as the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems.

The DHS/ALL-038 Insider Threat Program System of Records Notice (SORN)[3] was updated to cover records 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. Information maintained by the ITP now includes information lawfully

[2] The National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs that implements Executive Order No. 13587 define the terms "Insider Threat" and "Insider." While these definitions, read in isolation of EO 13587, appear to provide an expansive definition of the terms "Insider" and "Insider Threat;" the reforms mandated by EO 13587 are limited to protecting classified information from unauthorized disclosure, and thus so are these terms.
[3] DHS/ALL-038 Insider Threat Program System of Records, 85 FR 13914 (Mar. 10, 2020).

obtained from any United States Government Agency, DHS Component, other domestic or foreign government entity, and from a private sector entity.

Privacy Impact Analysis

Authorities and Other Requirements

Additional authorities not found in the previously published Insider Threat Program PIA include:

1. Office of the Director of National Intelligence, Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position;
2. DHS Directive 121-14, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position (Sept. 17, 2018);
3. DHS Instruction 262-05-002, Revision 01, Insider Threat Program (Oct. 1, 2019);
4. DHS Instruction 262-05-002-01, Insider Threat Information Sharing Guide (Oct. 11, 2019);
5. Intelligence Community Standard 500-27, Collection and Sharing of Audit Data;
6. Intelligence Community Standard 700-2, Use of Audit Data for Insider Threat Detection; and
7. Intelligence Community Standard 703-02, Reporting Requirements for Individuals with Access to SCI.

In addition to the authorities listed above, DHS updated DHS/ALL-038 Insider Threat Program SORN to account for the new population affected and the new types of information the program is now authorized to collect and maintain pursuant to the *Expanding the Scope of the Department of Homeland Security Insider Threat Program* memorandum approved on January 3, 2017.

Characterization of the Information

The ITP maintains information for the purposes of identifying, analyzing, or resolving insider threat matters. As part of this update, information available to the ITP may now come 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. Moreover, the ITP may access from any United States Government Agency, other domestic or foreign government entity, and from a private sector entity information lawfully obtained.

DHS is expanding the ITP data elements to include current employment and performance information, contract information, personnel files containing information about misconduct and adverse actions, and current and former security clearance status.

Privacy Risk: There is a risk of overcollection of employee information with the scope of the population being increased. Additionally, with the expanded scope, more information than necessary may be analyzed in order to determine if an actual insider threat exists.

Mitigation: This risk is partially mitigated. The DHS Insider Threat Operations Center's (ITOC) person-centric tool suite design combined with its unique filtering capabilities allow the ITP to share data with stakeholders with more complex access controls. For example, if there is a stakeholder that only has authority to receive information, either statutorily or through an information sharing agreement with the ITP, the tool suite can filter out records from the data the user receives. Furthermore, for stakeholders who are allowed to access ITP data, but must handle that data differently, the ITOC tool suite tags the data so the stakeholder can handle it appropriately.

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. 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 Insider Threat Oversight Group (ITOG) (which includes Office of the General Counsel (OGC), Office of Civil Rights and Civil Liberties (CRCL), and DHS Privacy Office (PRIV) representatives) to ensure compliance with applicable laws, regulations, and policies.

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—were created for a smaller population and do not account for the expanded scope.

Mitigation: This risk is partially mitigated. While the initial triggers did not contemplate potential workplace violence on the unclassified network by uncleared employees, 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 ITOC 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 Standard Operating Procedure (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 anomalous 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/Intelligence Law Division (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: There is a risk that ITOC data will become outdated and inaccurate, because the ITOC draws upon data aggregators from DHS, other federal agencies, other domestic or foreign government entities, and from private sector entities, to obtain data instead of collecting directly from individuals.

Mitigation: This risk is mitigated. 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[4] 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. Prior to any external disclosure of information, the ITP Manager and DHS OGC review all referrals to minimize the amount of information sent to the recipient to perform their official responsibilities. The ITOG monitors compliance with this requirement through quarterly audits as required by the ITOC SOP.

Uses of the Information

Originally, the ITP focused on the detection, prevention, and mitigation of unauthorized disclosure of classified information by DHS personnel with active security clearances. The Secretary's memorandum expands the scope of the ITP to its current breadth: threats posed to the Department by *all* individuals who have or had access to the Department's facilities, information, equipment, networks, or systems. Unauthorized disclosure of classified information is merely one way in which this threat might manifest.

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 ITOC's insider threat mission.

Privacy Risk: There is a risk that members of the ITOC will review data that is not relevant to analysis of insider threats. Some information compiled could be illegal activity but not within the scope of the ITP.

Mitigation: This risk is mitigated. 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

[4] *See* DHS/ALL/PIA-052(a) DHS Insider Threat Program Appendix A, *available at* www.dhs.gov/privacy.

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.

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.

Notice

The Insider Threat Program SORN, this PIA, the Privacy Act statements on Standard Forms, periodic notification to the workforce by email, and annual training required of all employees serve to provide notice to employees that information they provide to the U.S. Government and information legally obtained through user activity monitoring may be used by the ITOC to discern whether there is a threat to the Department by an insider. However, persons not directly employed by DHS may not receive notice by all of the methods the Department uses to create transparency.

Privacy Risk: There is a privacy risk that all persons who are not DHS employees may not be aware at the time of collection that he or she may be subject to user activity monitoring.

Mitigation: This risk is partially mitigated. Cleared individuals who have completed an SF-86 or employees in positions of public trust who have completed an SF-85 have been provided notice that their information will be used to determine if they might be an insider threat. All persons accessing DHS information technology are presented with banners informing them that access requires their consent to user activity monitoring.

Public notice is provided to all persons by the DHS/ALL-038 Insider Threat Program SORN and this PIA, but non-DHS personnel who use DHS facilities or resources are unlikely to encounter specific notification that information related to their activity at a DHS facility may be provided to the ITP.

For Components, the collecting agency is responsible for providing notice at the point of collection that the information may be shared with other federal, state, local, and foreign government agencies and authorized organizations following approved routine uses described in the associated published SORNs. Further, some collecting Components also provide notice through their published PIAs that the information collected may be shared with the ITP.

Data Retention by the project

No change from the previously published DHS Insider Threat Program PIA.

Information Sharing

No change from existing PIA in this area.

Redress

If an individual would like to file a Privacy Act or Freedom of Information Act (FOIA) request to view his or her record, he or she may mail the request to the new address:

Chief Privacy Officer/Chief Freedom of Information Act Officer
Department of Homeland Security
2707 Martin Luther King Jr. Avenue, SE
Washington, D.C. 20528
Phone: 202-343-1743 or 866-431-0486
Fax: 202-343-4011
E-mail: foia@hq.dhs.gov

These 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 "Contact Information." 6 CFR part 5, Subpart B, provides the rules for requesting access to Privacy Act records maintained by DHS.

Auditing and Accountability

No change from the previously published DHS Insider Threat Program PIA.

Responsible Officials

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

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
Department of Homeland Security