Privacy Impact Assessment

for the

DHS Counterintelligence Program

DHS Reference No. DHS/ALL/PIA-086

August 31, 2020

Homeland Security

Abstract

The U.S. Department of Homeland Security (DHS) Counterintelligence (CI) Program is a Department-wide effort designed to detect, deter, and disrupt foreign intelligence threats directed at the United States. CI encompasses those activities that identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents (including transnational criminal organizations and drug trafficking organizations conducting intelligence-related activities), or international terrorist organizations or activities, collectively hereinafter referred to as foreign intelligence entities (FIE).[1] DHS is conducting this Privacy Impact Assessment (PIA) because the DHS CI Program requires access to, collection of, and storage of personally identifiable information (PII) associated with individuals who are either involved in, witness to, or knowledgeable of CI-related activities that are the subject of inquiry by DHS, or supporting CI activities conducted by the DHS CI Program.

Overview

The DHS CI Program is a coordinated Department effort to detect, deter, and disrupt foreign intelligence threats directed at the United States. Within DHS, only two Components are members of the Intelligence Community (IC): the Office of Intelligence & Analysis (I&A) and the U.S. Coast Guard (USCG), which each have different authorities under Executive Order (EO) 12333 "United States Intelligence Activities" [2] (as well as through their own statutory authorities, which are explained in more detail below). As members of the IC, I&A and the USCG have a number of responsibilities to support the U.S. intelligence effort, under the leadership of the Director of National Intelligence (DNI).[3] In addition, the heads of elements of the IC are required to report to the Attorney General (AG) possible violations of federal criminal laws by employees and provide copies of all such reports to the Director concerning any intelligence activities.[4]

Office of Intelligence & Analysis (I&A)

Pursuant to DHS Delegation No. 08503,[5] the Under Secretary for Intelligence and Analysis

[1] Foreign Intelligence Entities (FIE) are known or suspected foreign state or non-state organizations or persons that conduct intelligence activities to acquire information about the United States, block or impair intelligence collection by the U.S. Government, influence United States policy, or disrupt systems and programs owned or operated by or within the United States. The term includes foreign intelligence and security services, international terrorists, transnational criminal organizations, and drug trafficking organizations conducting intelligence-related activities.
[2] Executive Order 12333, *United States Intelligence Activities*, 46 Fed. Reg. 59941 (Dec. 4, 1981), *as amended by* Executive Order 13470, *Further Amendments to Executive Order 12333, United States Intelligence Activities*, 73 Fed. Reg. 45325 (July 30, 2008).
[3] *Id.* at 1.4.
[4] *Id.* at 1.6(a)-(h).
[5] U.S. DEPARTMENT OF HOMELAND SECURITY, DELEGATION NO. 08503, DELEGATION TO THE UNDERSECRETARY FOR INTELLIGENCE AND ANALYSIS/CHIEF INTELLIGENCE OFFICER (2012), on file with the DHS Privacy Office.

(USIA) leads a unified DHS CI Program as the DHS Counterintelligence Executive (DCIX). Pursuant to DHS Delegation No. 08506,[6] the USIA, in his role as DCIX, delegated authority to the Counterintelligence Director (DCID) and the Department's Component Heads to exercise and fulfill counterintelligence authorities and responsibilities for the Department. The DHS CI Program protects against intelligence activities directed against the United States through the issuance of strategies, policies, procedures, guidelines, and standards relating to CI, and the tasking of Component heads as necessary to accomplish DHS CI objectives. The DHS CI Program consists of every Component CI Element (CCE)[7] from each of the DHS Components that engage in one or more of the following functions: CI investigations/inquiries, CI collections, CI operations, CI analysis, CI production, or CI functional services.[8]

DHS Instruction No. 264-01-002, "DHS Counterintelligence Program,"[9] establishes the DHS CI Program as part of an integrated national and Departmental effort to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents (including transnational criminal organizations and drug trafficking organizations conducting intelligence-related activities), or international terrorist organizations or activities. The DHS CI Program focuses on these FIE activities against DHS personnel, information, material, facilities, or activities.

U.S. Coast Guard (USCG)

The USCG Counterintelligence Service (CGCIS) is covered by this PIA but has slight variations in its policies and procedures due to its unique and separate authorities. USCG intelligence authorities are derived from Executive Order (EO) 13286, Amendment of EOs, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security, and Executive Order 12333, which authorizes the Commandant of the Coast Guard to conduct counterintelligence activities including through clandestine means. The primary distinction between the CGCIS and the rest of the DHS CI Program is its intelligence oversight guidelines. As required by EO 12333, the I&A Counterintelligence Mission Center (CIMC) and all the CCEs (other than the CGCIS) follow DHS I&A Instruction IA-1000, Office of Intelligence

[6] U.S. DEPARTMENT OF HOMELAND SECURITY, DELEGATION NO. 08506, DELEGATION OF COUNTERINTELLIGENCE FUNCTIONS WITHIN THE DEPARTMENT OF HOMELAND SECURITY (2020), on file with the DHS Privacy Office.
[7] As of May 2020, the DHS CI Program is made up of I&A, Cybersecurity and Infrastructure Security Agency (CISA), Countering Weapons of Mass Destruction (CWMD), Federal Emergency Management Agency (FEMA), Transportation Security Administration (TSA), U.S. Citizenship and Immigration Services (USCIS), U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Secret Service (USSS), and Federal Protective Service (FPS).
[8] U.S. DEPARTMENT OF HOMELAND SECURITY, INSTRUCTION NO. 264-01-002, REVISION 01, DHS COUNTERINTELLIGENCE PROGRAM (2017), on file with the DHS Privacy Office.
[9] *Id.*

and Analysis Intelligence Oversight Program and Guidelines[10] (I&A IO Guidelines), governing collection, retention, and dissemination of U.S. Persons (USPER) information and other specified counterintelligence activities. Because the USCG has distinct intelligence authorities, it has its own independent Commandant Instruction Manual 3820.12, Coast Guard Intelligence Activities[11] (COMDTINST M3820.12) vetted by the AG, and Commandant Instruction 3821.14, Oversight of Coast Guard Intelligence Activities (COMDTINST 3821.14), that establishes policies and procedures for the oversight of Coast Guard intelligence activities.[12] The additional counterintelligence authorities provided to the USCG are not further shared with the rest of the DHS CI Program, and are not restricted based on the limitations applied to I&A.

DHS CI Functions

Counterintelligence activities within the DHS CI Program (CIMC, CGCIS, and all other CCEs) are undertaken as part of an integrated national and departmental effort. The DHS CI Program, including CGCIS, follows the Intelligence Community model for conducting counterintelligence, as laid out in Intelligence Community Directive 750 (ICD 750)[13] and other National Counterintelligence Security Center (NCSC) guidance. The DHS CI Program conducts a variety of activities to fulfill its mission, including investigations, information collections, operations, analysis and production, and functional services that support these activities. DHS CI Program functions are divided into the categories outlined below. Not every CCE will perform all of the CI functions listed below. The CIMC and CGCIS currently perform all five CI activities.

CI Analysis & Production is the process of examining and evaluating intelligence or information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of a FIE and creating finished intelligence products incorporating counterintelligence analysis in response to known or anticipated counterintelligence concerns.

CI Collections involve the systematic acquisition of intelligence or information to answer

[10] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, INSTRUCTION NO. IA-1000, OFFICE OF INTELLIGENCE AND ANALYSIS INTELLIGENCE OVERSIGHT PROGRAM AND GUIDELINES (2017), *available at* https://www.dhs.gov/sites/default/files/publications/office-of-intelligence-and-analysis-intelligence-oversight-program-and-guidelines.pdf.

[11] U.S. COAST GUARD, COMMANDANT INSTRUCTION M3820.12, COAST GUARD INTELLIGENCE ACTIVITIES (2003) [hereinafter COMDTINST M3820.12], on file with the USCG Privacy Office. COMDTINST M3820.12 is currently being rewritten to provide new and updated standards that are consistent with other members of the intelligence community and the Department of Defense.

[12] U.S. COAST GUARD, COMMANDANT INSTRUCTION 3821.14, OVERSIGHT OF COAST GUARD INTELLIGENCE ACTIVITIES (2003) [hereinafter COMDTINST 3821.14], on file with the USCG Privacy Office. COMDTINST 3821.14 establishes policies and procedures for the oversight of Coast Guard intelligence activities and implements procedures for the conduct of intelligence oversight as required by Executive Order 12333 and Executive Order 13286.

[13] OFFICE OF DIRECTOR OF NATIONAL INTELLIGENCE, INTELLIGENCE COMMUNITY DIRECTIVE 750, COUNTERINTELLIGENCE PROGRAMS (2013), *available at* https://www.dni.gov/files/documents/ICD/ICD750.pdf.

national or Departmental counterintelligence collection requirements.[14]

CI Investigations are activities undertaken to determine whether a particular individual is conducting espionage, other intelligence activities, sabotage, or assassinations on behalf of a foreign power, FIE, foreign person, or international terrorist organization or agent thereof; and to determine actions required to exploit, disrupt, or protect against such acts.

CI Operations are activities designed to identify, exploit, disrupt, or deter FIE activities. CGCIS is the only DHS CCE that currently has the authority to conduct offensive counterintelligence operations (i.e., proactive efforts to exploit or disrupt FIE activities). The rest of the DHS CI Program, per EO 12333, are limited to defensive counterintelligence operations intended to identify and disrupt FIE activities aimed at DHS facilities, personnel, and missions. In addition, members of the DHS CI Program can support CI operations of other members of the U.S. Intelligence Community, in accordance with law and DHS policy.

CI Functional Services are activities that enable one or more of the other CI functions described above, including defensive CI activities, CI awareness, and reporting training (including threat awareness briefs, foreign travel briefs, and foreign visit briefs and debriefs); CI support to insider threat program[15] and mitigation efforts; CI support to research, development, and acquisition; supply chain risk management; and critical infrastructure protection; CI support to force protection; and cyber CI.[16]

Collection of PII

The DHS CI Program uses a combination of activities as a means of collecting information, including PII, to fulfill program responsibilities. The DHS CI Program collects PII directly from DHS employees and contractors via in-person interview, from individuals outside of DHS who may have relevant information for a CI matter, government-controlled and public data aggregators,[17] forensic examination of documents and electronic media, and anonymous tips and

[14] In the field of counterintelligence, a collection requirement is defined as "an established intelligence need validated against the appropriate allocation of intelligence resources (as a requirement) to fulfill the essential elements of information and other intelligence needs of an intelligence consumer." JOINT CHIEFS OF STAFF, JOINT PUBLICATION 2-01.2, CI AND HUMINT IN JOINT OPERATIONS (2011).

[15] The DHS Insider Threat Program has its own SORN and PIA, separate from the DHS CI Program. *See* DHS/ALL-038 Insider Threat Program System of Records, 85 Fed. Reg. 13914 (Mar. 10, 2020). *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE DHS INSIDER THREAT PROGRAM, DHS/ALL/PIA-052 (2015 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-department-wide-programs.

[16] *Generally* INTELLIGENCE COMMUNITY DIRECTIVE 750, *supra* note 13; INSTRUCTION NO. 264-01-002, *supra* note 8; U.S. COAST GUARD, COMMANDANT INSTRUCTION MANUAL M3850.1, COAST GUARD COUNTERINTELLIGENCE SERVICE (2008) (COMDTINST M3850.1), on file with the USCG Privacy Office.

[17] Data aggregation is any process in which information is gathered and expressed in a summary form, for purposes such as statistical analysis. A public data aggregator refers to a tool used to automatically search, combine, and display publicly available information concerning some topic in one location. The information itself is unclassified, open source, and is usually available on the Internet. There are also commercial data aggregators, run by

leads provided via email, telephone, and written notes or letters. Additional techniques and sources may be classified. The DHS CI Program uses this PII to support the program and its functions.

As it relates to CI investigations and operations, PII may be used to identify individuals who are involved in, witness to, or knowledgeable of CI-related activities that are the subject of a CI investigation or operation by the DHS CI Program or other federal law enforcement or intelligence agencies where there is a DHS equity. Additionally, the PII collected by the DHS CI Program is used to confirm or refute allegations against subjects of DHS CI investigations or operations who exhibit any of the CI indicators that may be associated with a potential espionage or international terrorist threat. CI indicators are included in Appendix A of this PIA.

CI analytical products generally contain very limited amounts of PII, with sources and individuals referenced in a finished intelligence product anonymized to the greatest extent possible. When the analytical product is not specifically about an individual or group of individuals, the product will generally mask the identity of the individuals referenced and note whether these individuals are USPER or foreign actors. For a product specifically about an individual, the product may contain PII and Sensitive PII, but will be protected in accordance with DHS intelligence oversight guidelines.[18]

The DHS CI Program also collects PII on DHS employees, contractors, and other individuals in the course of performing the variety of activities that are categorized under the CI Functional Services. For example, the DHS CI Program provides DHS employees with CI awareness training during which PII is collected directly from DHS employees in order to maintain a record of when CI awareness training was last received. When the DHS CI Program conducts digital forensics, the activities result in the collection of PII that the program uses to further identify individuals who are involved in (henceforth referred to as either a Subject or Subjects), witness to, or knowledgeable of CI-related activities being investigated by DHS Components or other federal law enforcement or intelligence agencies. The CI Program also conducts post foreign travel/foreign contact debriefings of DHS employees, which results in the collection of DHS employee PII, as well as certain information on individuals identified by the employee being debriefed. In cases in which an employee contacts the DHS CI Program in order to report that another employee is exhibiting suspicious behavior associated with counterintelligence indicators, PII is collected from the individual making the report, as well as on the subject of the claim. During

---

corporations which collect the information from publicly available and proprietary records. For this PIA, the terms public data aggregator and commercial data aggregator are used interchangeably. Examples of public and commercial data aggregators are: Lexis Nexis, Westlaw, Axciom, ChoicePoint, and Equifax. For DHS discussion of commercial data aggregators, *see* U.S. DEPARTMENT OF HOMELAND SECURITY, DATA PRIVACY & INTEGRITY ADVISORY COMMITTEE, REPORT NO. 2006-03, THE USE OF COMMERCIAL DATA (2006), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_commdata.pdf.

[18] The majority of the DHS CI program will fall under INSTRUCTION NO. IA-1000, *supra* note 10; the exception will be the USCG, which follows COMDTINST 3821.14, *supra* note 12.

a CI Investigation, the DHS CI Program routinely collects PII from government-controlled and commercial data aggregators to confirm or refute a Subject's association with potential espionage or international terrorist threats.

Privacy Protection and Risk Mitigation

The DHS CI Program has taken steps to protect privacy and mitigate the risk of misusing PII by creating a centralized and managed cross-domain (Unclassified and Classified networks) information management sharing system, referred throughout this document as the Counterintelligence Information Management System (CIIMS), to retain information collected from the conduct of DHS CI Program activities. Due to the sensitive nature of the PII collected and retained, CIIMS is virtually separated from the DHS computing environment such that system administrators (including privileged users) that monitor other DHS systems are blocked from accessing the tools, data, and information available to the DHS CI Program. Only the CIIMS system administrators and authorized users are able to access the tools, data, and information in CIIMS. CIIMS is not connected to any other system, either outside or inside DHS. Presently, this information sharing system is not yet available to all DHS CI Program personnel.[19] This technical solution, when fully adopted, will serve to ensure the confidentiality and integrity of the sensitive PII maintained by the DHS CI Program. Until the system is fully available to all DHS CI Program personnel, the DHS CI Program also stores all information on secure, access-controlled Departmental shared drives that are restricted to personnel of the DHS CI Program.

Additionally, all DHS CI Program personnel receive annual specialized training from the I&A Intelligence Oversight (IO) Officer regarding the collection, use, dissemination, and retention of USPER information, to include PII.[20]

DHS CI Program information is shared with DHS Components (beyond the staff involved in the CCE), the U.S. Intelligence Community, federal law enforcement agencies, and state, local, territorial, tribal, and private sector (SLTTP) partners on a need-to-know basis in order to protect against FIE activities designed to exploit or harm DHS equities and in accordance with the Routine Uses outlined in the DHS/I&A-001 I&A Enterprise Records System (ERS) system of records notice (SORN) and the forthcoming DHS/ALL-046 Counterintelligence Program System of Records, which will provide more sufficient notice of how DHS collects and maintains records as part of the unified Counterintelligence Program across the Department.[21] The dissemination of intelligence information about USPERs by the DHS CI Program is governed by DHS I&A

[19] Information that cannot be stored at this time in the CIIMS system is stored on an Authority to Operate-approved network.
[20] Because USCG has different Intelligence Oversight guidelines from the rest of the DHS CI Program, USCG personnel receive annual specialized training from USCG Intelligence Oversight officials regarding the collection, use, dissemination, and retention of USPER information.
[21] *See* DHS/IA-001 Enterprise Records System (ERS), 73 Fed. Reg. 28128 (May 15, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns.

Instruction No. IA-1000, "Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines,"[22] which was approved by the AG, pursuant to Executive Order 12333, "United States Intelligence Activities."[23]

Pursuant to DHS I&A Instruction No. IA-1000, the originator of an intelligence product has 180 days[24] from the date of collection of USPER data to determine whether it is necessary for the furtherance of an authorized national or Departmental mission, and if the collected information is reasonably believed to fall within one of the authorized information categories. If the collected data does not meet both requirements, the records are to be disposed of immediately, but no later than 180 days from date collected.[25]

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?

Executive Order 12333 – United States Intelligence Activities

The DHS CI Program derives its counterintelligence authorities from a range of sources, but the two primary sources are EO 12333 - United States Intelligence Activities[26] and the Homeland Security Act.[27] Under EO 12333, the President of the United States, by the authority vested in him by the Constitution and statute, including National Security Act of 1947,[28] as amended, provides guidance for the operation of the U.S. intelligence effort. The primary goal of EO 12333, and of the U.S. intelligence effort, is to provide the President, the National Security Council (NSC), and the Homeland Security Council with the necessary information on which to base decisions concerning the development and conduct of foreign, defense, and economic policies, and the protection of U.S. national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal.[29] Intelligence collection under this order is

[22] INSTRUCTION NO. IA-1000, *supra* note 10.
[23] *See* Executive Order 12333, *supra* note 2. The dissemination of intelligence information about USPER by the Coast Guard is governed by COMDTINST M3820.12, which is approved by the Attorney General pursuant to Executive Order 12333.
[24] With respect to USCG and pursuant to COMDTINST M3820.12, USCG originators of intelligence products have 90 days from the date of collection of USPER data to determine whether the information may be permanently retained within the USCG authorized procedures. The updated instruction will allow up to five years to determine if the USPER data may be permanently retained that is in alignment with other members of the intelligence community, the Department of Defense, and Presidential Policy Directive (PPD)-28.
[25] The USCG will dispose of all USPER data that does not meet requirements within 90 days of collection. Once the new instruction is promulgated, the USCG will dispose of all USPER data that does not meet requirements within five years of collection in accordance with COMDTINST M3820.12.
[26] Executive Order 12333, *supra* note 2.
[27] The Homeland Security Act of 2002, (Pub. L. 107–296, 116 Stat. 2135, Nov. 25, 2002), as amended.
[28] The National Security Act of 1947, (Pub. L. 235; 61 Stat. 496, July 26, 1947), as amended.
[29] Executive Order 12333, *supra* note 2, at 1.1.

guided by the need for information to respond to intelligence priorities set by the President,[30] with special emphasis given to detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; and (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction.[31] The DHS CI Program focuses its efforts on the first of the above special emphasis areas, detecting and countering espionage and other threats and activities directed by foreign powers or their intelligence services (i.e., conducting counterintelligence).

While all means consistent with applicable federal law and EO 12333 are permitted to obtain reliable intelligence information, the EO commits to a solemn obligation to conduct the intelligence activities under this EO in such a way as to protect fully the legal rights of all U.S. Persons, including their freedoms, civil liberties, and privacy rights guaranteed by federal law.[32]

As members of the IC, both I&A and the USCG are tasked with collecting information concerning and conducting activities to protect against intelligence activities directed against the United States by foreign powers, organizations, persons, and their agents.[33] I&A and USCG are expected to protect the security of intelligence related activities, information, installations, property, and employees by appropriate means, including such investigations of applicants, employees, contractors, and other persons with similar associations with the IC elements as are necessary.[34] These activities form the core of the Department's counterintelligence functions.

While all IC members are expected to perform the above counterintelligence functions, the method in which they are permitted to collect information differs. Some IC members are only permitted to conduct "overt or publicly available" collection activities while others are also permitted to engage in "clandestine" collection activities. Per EO 12333 1.7(i), I&A is allowed to collect (overtly or through publicly available sources), analyze, produce, and disseminate information, intelligence, and counterintelligence to support national and departmental missions.[35] In contrast, per EO 12333 1.7(h), the Intelligence and Counterintelligence Elements of the Coast Guard are permitted to collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence including defense and defense-related information and intelligence to support national and departmental missions.[36] Therefore, per EO 12333, USCG is permitted to collect foreign intelligence and counterintelligence using clandestine means, while I&A is only permitted to collect from overt or publicly available sources.

[30] *Id.* at 1.1(c).
[31] *Id.* at 1.1(c)-(d).
[32] *Id.* at 1.1(a) and (b).
[33] *Id.* at 1.4(b).
[34] *Id.* at 1.4(f).
[35] *Id.* at 1.7(i).
[36] *Id.* at 1.7(h).

In addition to the above-mentioned authorities, USCG is also authorized to "conduct counterintelligence activities,"[37] which include such actions as conducting offensive counterintelligence operations. In contrast, the I&A counterintelligence capability is focused on protecting against foreign intelligence activities.[38]

While I&A and USCG have different collection authorities, both I&A and USCG are able to use information legally collected by other members of the IC and members of the Executive Branch (including non-IC members and members of the Department of Defense), as well as from SLTTP partners.

Departmental Authorities to Conduct Counterintelligence Activities

Per the Homeland Security Act Section 201, codified at 6 U.S.C. § 121, the Under Secretary for Intelligence and Analysis is the Chief Intelligence Officer for the Department and has broad responsibility relating to intelligence and analysis.[39] This includes providing intelligence and information analysis and support to other elements of the Department;[40] establishing the intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines, and procedures for the intelligence components of the Department;[41] and other duties relating to such responsibilities as the Secretary may provide.[42]

Through DHS Delegation No. 08503,[43] the Secretary delegated to the Under Secretary for Intelligence and Analysis the authority to serve as the Secretary's representative to the National Counterintelligence Executive, the National Counterintelligence Policy Board created by Title 50, U.S.C. § 402a, "Coordination of Counterintelligence Activities,"[44] and other national counterintelligence community forums.[45] Delegation No. 08503 also delegates to the USIA the authority to "lead a unified DHS Counterintelligence Program as the DHS Counterintelligence Executive, including by conducting activities to protect against intelligence activities directed against the United States, issuing strategies, policies, procedures, guidelines, and standards relating to CI, and tasking Component heads as necessary to accomplish DHS CI objectives."[46]

DHS Instruction No. 264-01-002[47] establishes a comprehensive, integrated, and unified CI Program across DHS, under the authority of the Under Secretary for Intelligence and Analysis/

[37] *Id.*
[38] *Id.* at 1.4(b), (f), 1.7(i).
[39] 6 U.S.C. § 121.
[40] *Id.* § 121(d)(15).
[41] *Id.* § 121(d)(17).
[42] *Id.* § 121(d)(22).
[43] DELEGATION NO. 08503, *supra* note 5.
[44] *Id.* at II.B.
[45] *Id.* at II.A.
[46] *Supra* note 44.
[47] INSTRUCTION NO. 264-01-002, *supra* note 8.

DHS Chief Intelligence Officer (CINT), in his or her delegated role as the DCIX.[48] This instruction also charges the DCIX to "[task] Component Heads to accomplish DHS CI objectives, including by requiring access to Component datasets, records, information, and processes, as appropriate."[49]

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

The DHS/I&A-001 I&A Enterprise Records System (ERS) SORN[50] provides interim coverage for all records and information collected, maintained, disseminated, or used by the DHS CI Program to provide intelligence and analysis support to DHS. The forthcoming DHS/ALL-046 Counterintelligence Program System of Records will provide more sufficient notice of how DHS collects and maintains records as part of the unified Counterintelligence Program across the Department. Any records created by DHS Components under the CI program remain under the centralized control of I&A. The exception is the USCG, which conducts intelligence activities under its own EO 12333 authorization and which retains control of its own records. Pending finalization of the Counterintelligence SORN, the primary SORN for the USCG CI program is DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder.[51]

These records are used by the DHS CI Program to cull, analyze, and fuse intelligence and related information received from across the DHS Intelligence Enterprise; other federal departments and agencies (including law enforcement agencies); elements of the IC; and foreign, state, local, territorial, tribal, and private sector partners. ERS covers both classified and unclassified information.

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

An updated Authority to Operate (ATO) for the DHS CI Program and its cross-domain information management system (CIIMS) is approved through September 30, 2020. This ATO and the system security plan will be updated upon completion of this PIA.

---

[48] The responsibility of the CINT to lead the DHS Counterintelligence Program is also found in DHS Directive No. 264-01. U.S. DEPARTMENT OF HOMELAND SECURITY, DIRECTIVE NO. 264-01, INTELLIGENCE INTEGRATION AND MANAGEMENT (2013), on file with the DHS Privacy Office.

[49] This requirement for DHS Components to support the CINT in his intelligence role is consistent with 6 U.S.C. § 124d (2), (7) and DHS Directive 264-01-002. INSTRUCTION NO. 264-01-002, *supra* note 8, at IV(B)-(C); 6 U.S.C. § 124d (2), (7).

[50] DHS/IA-001 Enterprise Records System (ERS), *supra* note 21.

[51] *See* DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder, 73 Fed. Reg. 56930 (Sept. 30, 2008), *available at* https://www.dhs.gov/system-records-notices-sorns

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

Yes. The NARA approved records schedule N1-563-08-4-1[52] applies to DHS CI Program records. CI investigative files are temporary records and must be cut off[53] when an investigation is complete and the case is closed. The CI Investigative file records must be destroyed 20 years after cut-off. Other federal agencies may send copies of counterintelligence reports for reference to current DHS cases or the case files may contain "derivative memos" that describe a threat assessment compiled by outside sources.

NARA approved records schedule N1-563-07-16[54] also applies to DHS CI Program Records. Dissemination files and lists are temporary records and must be cutoff at the end of the calendar year. Dissemination files and list records must be destroyed or deleted two years after cut-off. Raw reporting files are temporary records and must be cut off at the end of a calendar year. Raw reporting file records must be destroyed or deleted 30 years after cut-off. Finished intelligence case files are permanent records and must be cut off at the end of the calendar year in which a case is closed. Finished intelligence case files are permanent records and must be transferred to the National Archives 20 years after cut-off.

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 DHS CI Program does not collect information covered by the PRA.

Section 2.0 Characterization of the Information

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

The DHS CI Program collects, uses, disseminates, and maintains a variety of PII including: biographic information; biometric data, including facial images and fingerprints;

---

[52] *See* U.S. NATIONAL ARCHIVES & RECORDS ADMINISTRATION, GENERAL RECORDS SCHEDULE N1-563-08-4-1, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-08-004_sf115.pdf (last visited July 23, 2020).

[53] Defined by NARA as the breaking or ending of files at regular intervals, usually at the close of a fiscal or calendar year, to permit their disposal or transfer in complete blocks and, for correspondence, to permit the establishment of new files.

[54] *See* U.S. NATIONAL ARCHIVES & RECORDS ADMINISTRATION, GENERAL RECORDS SCHEDULE N1-563-07-16, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/n1-563-07-016_sf115.pdf (last visited July 23, 2020).

contact information; Social Security number; passport information; citizenship; security clearance information to include background investigation information; reports of criminal, civil, and financial actions taken against an individual; medical history; level of education; travel history; and other information that is used by members of the IC to meet essential mission requirements.

The DHS CI Program may collect information related to individuals who are known, reasonably believed to be, or are suspected of being involved in or linked to the intelligence gathering activities of FIE; international terrorism; and transnational organized crime (including transnational drug trafficking organizations). Information may also be collected from individuals who are providing information related to the possible/suspected involvement of other DHS employees, whether voluntary or involuntarily, in intelligence activities of a foreign power.[55] A more expansive explanation of the types of information collected, used, disseminated, and maintained by the DHS CI Program can be found in Appendix B of this PIA.

The DHS CI Program also collects, uses, disseminates, and maintains classified and unclassified intelligence, counterterrorism, homeland security, and related law enforcement information, including source records and the reporting and results of any analysis of this information. Information may be obtained from all agencies, components, and organizations of the federal government, including the IC; foreign governments, organizations, or entities; international organizations; state, local, tribal, and territorial government agencies (including law enforcement agencies); and private sector entities.

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

The DHS CI Program collects information from individuals; DHS components; other government (federal, state, local, tribal) departments and agencies; non-government organizations; commercial parties; public institutions; private groups (both domestic and foreign); media (including periodicals, newspapers, broadcast transcripts, online media, and publicly available social media); intelligence source documents; anonymous tips and leads provided via email, telephone, and written notes or letters; and investigative reports and correspondence. Sources of information are cataloged, and if used for an intelligence product, a source statement is appended to the product.

Information collected from sources other than an individual (i.e., information from a system) is required to:

[55] The DHS CI Program works closely with the DHS Office of the Chief Security Officer (OCSO), the DHS Office of the Inspector General (OIG), and Component Security or Intelligence offices, as appropriate. However, DHS CI does not have full access to these office's records or files, and instead receives referrals of matters, or coordinates on cases, as appropriate, and consistent with each office's own SORNs and routine uses.

- Further identify individuals who are:
    - Involved in, witness to, or knowledgeable of CI-related activities that are the subject of an investigation by DHS components or other federal law enforcement or intelligence agencies; or
    - Supporting CI activities conducted by the DHS CI Program.
- Determine whether a particular individual is associated with a FIE.
- Confirm or refute allegations against individuals who exhibit any of the behaviors that may be associated with a potential espionage or international terrorist activity that may pose a threat to the Department or U.S. Persons or property.

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. The DHS CI Program obtains data from commercial sources and publicly available information (such as social media) in order to complement, clarify, or provide context to data from internal DHS sources. Commercially available data and publicly available electronic information is collected on individuals to clarify or resolve suspected FIE involvement. Records are also obtained from public financial disclosure reports and media, including periodicals, newspapers, and broadcast transcripts. Information from commercial sources or publicly available are not used to make sole determinations.

2.4 Discuss how accuracy of the data is ensured.

The DHS CI Program uses information provided by the individual (subject or reporter), and a variety of available data sources, to verify and corroborate information to the greatest extent possible. The accuracy of DHS-owned data, other federal agency data, and data provided by commercial data aggregators and publicly available sources is dependent on the original source. The DHS CI Program requires that all DHS CI Program personnel fully attribute individual information to the individual or system that provided such information. The DHS CI Program employs an auditing, peer review, legal oversight, and intelligence oversight process to ensure that data is accurate. Additionally, CI Program personnel will report data inaccuracies to the underlying DHS system from which the data was obtained in order to facilitate its correction. The accuracy of information from commercial data aggregators and publicly available sources is vetted by DHS CI Program personnel for accuracy by cross-checking the information against multiple sources.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a privacy risk that the among the large quantities of information that the DHS CI Program collects in order to identify information of value, a significant portion may not likely have any ultimate CI value.

Mitigation: This risk is partially mitigated. The IC value of information cannot be determined until after it is collected and analyzed. While the DHS CI Program may collect a wide variety of information from individuals reporting potential FIE intelligence activities, as well as individuals who are the subject of investigations, only PII necessary to conduct CI-related activities is retained. The DHS CI Program uses the collected PII to confirm or refute whether a particular individual is conducting espionage, other intelligence activities, sabotage, or assassinations on behalf of a foreign power, foreign organization, foreign person, or international terrorist organization or agent thereof; and to determine actions required to exploit, disrupt, or protect against such acts. The DHS CI Program minimizes the risk of collecting more information than is necessary by focusing on counterintelligence indicators.

Additionally, CI analytical products generally contain very limited amounts of PII, with sources and individuals referenced in a finished intelligence product anonymized to the greatest extent possible. When the analytical product is not specifically about an individual or group of individuals, the product will generally mask the identity of the individuals referenced and note whether these individuals are USPER or foreign actors.

Privacy Risk: There is a risk that the DHS CI Program's use of data aggregators from DHS, other federal agencies, and commercial entities to obtain data, instead of always collecting directly from individuals, will result in the use of outdated or inaccurate information.

Mitigation: This risk is partially mitigated. Through the DHS CI Program's analysis process, which relies heavily on the review of both historic and current information in order to establish patterns, it highlights discrepancies in information between different databases. The identification of those discrepancies allows the CI Program to draw a comparison between past and present behavior, as well as confirm or refute the veracity of information held within DHS CI Program records.

Privacy Risk: There is a privacy risk that DHS CI Program users could make decisions based on incorrect or biased information. DHS CI Program personnel are permitted to conduct their own analysis and incorporate data from commercial data aggregators and publicly available sources, rather than using only directly collected information. Information provided by those sources could prove to be incorrect or biased.

Mitigation: This risk is mitigated. The DHS CI Program requires that all DHS CI Program

personnel fully attribute individual information to the individual or system that provided such information. The DHS CI Program employs an auditing, peer review, legal oversight, and intelligence oversight process to ensure that data is accurate. The accuracy of information from commercial data aggregators and publicly available sources is vetted by DHS CI Program personnel for accuracy by cross-checking the information against multiple sources. DHS CI Program personnel report data inaccuracies to the underlying DHS system from which it was obtained in order to facilitate its correction.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

The DHS CI Program uses PII and the other information that it collects to further identify individuals who are either involved in, witness to, or knowledgeable of CI-related activities that are the subject of an investigation by DHS Components or other federal law enforcement or intelligence agencies; or that supports CI activities conducted by the DHS CI Program. Additionally, the DHS CI Program collects PII to confirm or refute allegations against individuals who exhibit any of the behaviors associated with a potential espionage or international terrorist threat. The collection of this information allows DHS CI Program personnel to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of FIEs.

Although CIIMS is not electronically connected to any other system, either outside or inside DHS, information is shared with DHS Components, the U.S. IC, other law enforcement agencies, and SLTTP partners in accordance with the DHS I&A Instruction No. IA-1000[56] and USCG COMDTINST M3820.12.[57] The ERS SORN and USCG LEIDB/Pathfinder SORN, which together provide interim coverage for the DHS CI program, allow such external sharing in accordance with the published routine uses as detailed below in Section 6.2. DHS is in the process of publishing the DHS/ALL-046 Counterintelligence Program System of Records SORN, which will provide more sufficient notice of how DHS collects and maintains records as part of the unified Counterintelligence Program across the Department.

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.

The DHS CI Program currently has no capability to discover or locate a predictive pattern

[56] INSTRUCTION NO. IA-1000, *supra* note 10.
[57] COMDTINST M3820.12, *supra* note 11. COMDTINST M3820.12 is approved by the Attorney General pursuant to Executive Order 12333.

or an anomaly using electronic searches, queries, or analyses of electronic databases. However, some of the source systems may have this capability; any such capability is described in the relevant Component PIAs. The DHS CI Program intends to develop this capability for the narrowly defined purpose of identifying anomalies that correspond to counterintelligence indicators as defined in Appendix A and predictive patterns to identify vulnerabilities of DHS and HSE equities that are at risk from FIE exploitation efforts.

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

Yes. The DHS CI Program consists of every CCE within the Department. CCEs are counterintelligence elements that engage in one or more or the following functions: CI investigations/inquiries, CI collections, CI operations, CI analysis and production, or CI functional services. Access to CIIMS has layers of authorization which include division firewalls, organizational hierarchy, role-based access controls, and file specific restricted access. Division firewalls create firewalls around user groups, preventing access and visibility to information from other user groups, such that by default a USCG user cannot see a U.S. Citizenship and Immigration Services (USCIS) product and vice versa. Organizational hierarchy ensures that, where there is a hierarchy consisting of district field offices, regions made up of districts and a headquarters element, regions cannot view products from other regions, and districts cannot view products from other districts. However, if it is determined there is a need-to-know, limited access can be granted across divisional firewalls and organizational hierarchies. Within both division firewalls and organizational hierarchies, access to products and files is further restricted through role-based access controls and, where necessary, file specific restricted access. Role-based access controls within CIIMS for individual DHS components are created based on an initial consultation with the Component administrator, who provides the CIIMS administrator with a list of users and the users' role (e.g., supervisor, analyst, CI officer) which are then defined in the system. Restrictions are created based upon these roles, such that, if a supervisor assigns an analyst to a particular group, the analyst can only see cases and files related to that particular groups' activities. CIIMS has an additional feature that allows administrators to restrict particularly sensitive products and files to certain assigned personnel only.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is a risk that data collected for the CI mission will be used for a purpose other than the originally stated purpose for which it was collected.

Mitigation: This risk is mitigated. Training of DHS CI Program personnel familiarizes them with the risks and consequences associated with the misuse of the data, which includes up to the loss of security clearance and/or employment. Additionally, the allowable uses and dissemination of information collected and maintained by the DHS CI Program is outlined in the

Routine Use portion DHS/I&A-001 I&A Enterprise Records System (ERS) SORN.[58] As such, information is shared with DHS components, the U.S. IC, other law enforcement agencies, and SLTTP partners on a case-by-case basis, with a demonstrated need-to-know. DHS CI Program dissemination of information about USPERs is governed by DHS I&A Instruction No. IA-1000,[59] which is approved by the Attorney General pursuant to Executive Order 12333, "United States Intelligence Activities."[60] DHS is in the process of publishing the DHS/ALL-046 Counterintelligence Program System of Records SORN, which will provide more sufficient notice of how DHS collects and maintains records as part of the unified Counterintelligence Program across the Department.

Privacy Risk: When information is gathered to assess whether a CI concern 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 CI program. For example, an analysis of information could result in the CCE discovering a criminal or administrative violation that must be reported to another entity, such as the DHS Office of Inspector General (OIG) or Federal Bureau of Investigation (FBI).

Mitigation: This risk is mitigated. Within CI activities, CI investigations are concerned with the federal crimes of espionage, terrorism, treason, subversion, sedition, and sabotage, as well as the mishandling of national defense information. DHS CI Program dissemination of information about USPERs is governed by DHS I&A Instruction No. IA-1000.[61] This requirement partially mitigates the concern arising from an investigation collecting information outside of the scope of the Department's CI Program by requiring immediate notification of oversight entities. The DHS CI Program's information sharing system, CIIMS, is not connected to any other system, either outside or inside DHS. However, processes are in place to enable the appropriate CCE to refer cases to the DHS OIG, FBI, or other law enforcement partners as appropriate, and securely transfer the information collected as part of that investigation.

Privacy Risk: There is a risk that personnel authorized to access DHS CI Program information could use their access for unapproved or inappropriate purposes, such as performing searches on themselves, supervisors, or coworkers.

Mitigation: This risk is mitigated. The DHS CI Program uses monitoring and analytic software to perform auditing that records the activities of all users. These audit logs are reviewed periodically by CIIMS system administrators and supervisors and any inappropriate use will be

[58] DHS/IA-001 Enterprise Records System (ERS), *supra* note 21. The primary SORN for the USCG CI program is DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder, *supra* note 52.
[59] INSTRUCTION NO. IA-1000, *supra* note 10.
[60] Executive Order 12333, *supra* note 2. The USCG CI program's dissemination of information about USPER is governed by COMDTINST M3820.12, which is approved by the Attorney General pursuant to Executive Order 12333.
[61] INSTRUCTION NO. IA-1000, *supra* note 10. The USCG is governed by COMDTINST M3820.12.

referred to the appropriate internal investigators (such as the DHS OIG or others as required) for handling. Any detection of potentially inappropriate system use will result in the suspension of a DHS CI Program user's access until the activity can be investigated and resolved.

The CIIMS system administrators and supervisors can conduct audits on the authorized users of CIIMS if a problem or concern arises regarding the use or misuse of information. When users log in, they must acknowledge and consent to monitoring before access will be provided.

Privacy Risk: There is a privacy risk that information obtained from multiple systems, including commercially available information, may not generally be indicative of CI activity and could be taken out of context.

Mitigation: This risk is partially mitigated. The DHS CI Program minimizes the risk of taking information out of context by focusing on counterintelligence indicators. DHS CI Program personnel use the imported data, as well as any analytical software tools,[62] to identify individuals, associations, or relationships associated with FIE. DHS CI Program data obtained from commercial sources is used to complement, clarify, or provide context to data from internal DHS sources. Information that is not necessarily indicative of derogatory information (DI) is used to refute a FIE nexus. The lack of this information would create a bias against an individual for whom a FIE nexus does not exist.

Privacy Risk: There is a privacy risk related to the compilation of data from multiple systems, as it provides users with access to information from several systems to which they would not normally have access to.

Mitigation: This risk is mitigated. The DHS CI Program minimizes the risk of compiling data that does not fall within the scope of the DHS CI Program through both training and policy. CI Officers are required to have formal training on the proper collection and retention of information. In addition, Appendices A and B of DHS Instruction No. 264-01-002 contain both CI indicators and a list of significant CI matters that DHS CI Program members use to evaluate whether information falls within the scope of the DHS CI Program.

[62] In reference to the analytical tools, CIIMS' analytical capability is designed to enable users to identify obvious and non-obvious relationships among entities as well as understand those organizational relationships within an existing record of information or within a case. The capability has an entity resolution functionality that identifies commonalities within data to suggest a common linkage and relationship. The functionality consolidates information into one point, provides record linking, record matching, and identifies and reduces duplication within a record. The user then reviews the consolidated record to determine whether a relationship exists and whether there's a valid association to existing information within their case.

Section 4.0 Notice

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

When DHS CI Program members collect information directly from individuals as part of an investigation, that collection is preceded by a Privacy Act Statement or Privacy Notice, as appropriate. Additionally, the ERS SORN[63] provides notice to the public on all records and information used by I&A to provide intelligence and analysis support to the DHS. This PIA, and the forthcoming CI SORN, further provides the public with notice of the ways in which information is collected and used by the DHS Counterintelligence Program.

Notice of USCG's CI efforts is provided by the LEIDB/Pathfinder SORN.[64]

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

Pursuant to 5 U.S.C. § 552a(e)(3) of the Privacy Act, the DHS CI Program provides a Privacy Act Statement or Privacy Notice before collecting PII directly from an individual. Privacy Act Statements and Privacy Notices provide notification of the authority (whether granted by statute or by executive order of the President) under which the information is being solicited; whether disclosure of such information is mandatory or voluntary, as well as the effects on an individual should they choose not to provide it; the principal purpose for which the information is intended to be used; and the uses which may be made of the information. In the cases in which information is collected directly from an individual, DHS CI Program personnel provide notification that offering such information is voluntary, but for security clearance holders, failure to comply with statutory and policy requirements regarding mandatory disclosure can impact that individual's security clearance. Currently, the DHS CI Program has approved Privacy Act Statements and Privacy Notices for CI Debriefings of Cleared Personnel, CI Debriefings of Personnel without a Clearance, and CI investigations.

Each of the various source systems that perform the original collection, and from which the DHS CI Program draws information, are subject to specific notice requirements and mechanisms for such notification. The ERS and USCG SORNs and this PIA provide additional notice. Additionally, the source systems from which the DHS CI Program 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

[63] DHS/IA-001 Enterprise Records System (ERS), *supra* note 21.
[64] DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder, *supra* note 52.

intelligence authority. As such, individuals may not have an opportunity to decline to provide the required information, opt out, or to consent to uses. Further, the DHS CI Program does not have the ability to provide individuals with the opportunity to consent to use or decline to provide information to commercial or publicly available sources because it does not control those systems and cannot provide notice other than through this PIA.

In cases in which an individual is providing the PII of another individual whom he or she suspects is involved in a counterintelligence matter, there is no ability to provide the subject of the investigation with notice.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a privacy risk that the DHS CI Program does not always collect information directly from the subject of the investigation. Therefore, the subject may not have notice that his or her information is used by the DHS CI Program.

Mitigation: This risk is partially mitigated. Notice is provided by this PIA, the ERS and USCG SORNs, and the forthcoming CI SORN, which outline the types of, and uses for, information that is collected or shared with the homeland security community for law enforcement or intelligence purposes. The ERS and USCG SORNs provide general notice to the public on the categories of individuals on whom information is collected, the types of information maintained, the purposes for the collection, and the routine uses for information when disclosed outside of DHS. Although the SORNs note that these systems of records have been exempted from notification, access, and redress to the extent permitted under subsection (k) of the Privacy Act,[65] they provide information on how the public can gain access and request redress of any non-exempt records.

Providing specific notice to individuals that are the subject of a CI investigation or effort would notify the individual that he or she is the focus of DHS efforts, potentially permitting him or her to impede government efforts to protect homeland security; reveal sensitive methods or confidential sources used to acquire the relevant information; or possibly implicate a potential law enforcement investigation and permit the individual to impede the investigation.

Section 5.0 Data Retention by the project

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

The DHS CI Program collects extensive PII to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of FIE, or activities directed against U.S. national security interests or DHS and its personnel, information, material, facilities, and activities. The DHS CI Program maintains this

[65] 5 U.S.C. § 552a(k).

information in either an active status or inactive status in accordance with the ERS SORN (the LEIDB/Pathfinder SORN in the case of USCG), the forthcoming CI SORN, and source system SORNs related to the information collected at the point of collection.

The retention period for the information collected by the DHS CI Program varies depending on the type of data. CI investigative records are temporary and must be cut off[66] when an investigation is complete, and the case is closed. CI investigative records are temporary and must be destroyed 20 years after cut-off. Raw reporting files are temporary and must be cut off at the end of a calendar year. Raw records are temporary and must be destroyed or deleted 30 years after cut-off. Finished intelligence case files are permanent and must be cut off at the end of the calendar year in which a case is closed. Finished intelligence records are permanent and must be transferred to the National Archives 20 years after cut-off. Interception, monitoring, and recording of wire and oral communication records are temporary, must be cut off at the end of the calendar year, and are destroyed 10 years after cut -off. Non-referral files are temporary and are destroyed five years old from first collected. Certification files are temporary and are to be destroyed when 10 years old or 10 years after completion of a specific training program or upon separation or transfer of employee, whichever is sooner. Mission-related training records are temporary and are destroyed or deleted 30 years after cutoff date.

Pursuant to the DHS I&A Instruction No. IA-1000, "Office of Intelligence and Analysis Intelligence Oversight Program and Guidelines," the originator of an intelligence product has 180 days from the date of collection of USPER data to determine whether it is necessary for the conduct or furtherance of an authorized I&A intelligence activity national or Departmental mission, and if the collected information is reasonably believed to fall within one of I&A's authorized collection information categories.[67]

If the collected data does not meet both requirements, the records are to be disposed of immediately, but no later than 180 days[68] from date collected. If the USPER data does meet both

[66] NARA guidelines on records management recommend that records in a series or system should be cut off, or broken, at regular intervals, usually annually, to permit their disposal or transfer in complete blocks and, for correspondence files, to permit the establishment of new files. Cutoffs are needed before disposition instructions can be applied because retention periods usually begin with the cutoff, not with the creation or receipt, of the records. *See* NATIONAL ARCHIVES & RECORDS ADMINISTRATION, DISPOSITION OF FEDERAL RECORDS: A RECORDS MANAGEMENT HANDBOOK 31-32 (2000), *available at* https://www.archives.gov/files/records-mgmt/pdf/dfr-2000.pdf.

[67] Pursuant to COMDTINST M3820.12, USCG originators of intelligence products have 90 days from the date of collection of USPER data to determine whether the information may be permanently retained within the USCG authorized procedures. The updated instruction will allow up to five years to determine if the USPER data may be permanently retained that is in alignment with other members of the intelligence community, the Department of Defense, and PPD-28.

[68] The USCG will dispose of collected data no later than 90 days if requirements are not met under the current instruction. The USCG will dispose of collected data no later than five years if requirements are not met under the revised instruction.

requirements, the records must be reviewed annually to determine whether there is still a mission need to retain the data. At the anniversary date (or any time beforehand), a record must be reviewed and verified to determine that a mission need remains that requires the data to be retained. This review cycle can occur indefinitely, so long as there remains a mission need to retain the data.

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is a privacy risk that the DHS CI Program may retain information about persons who are suspected of being CI threats without resolving whether the CI matter was upheld or vacated by an investigative component or agency, or for longer than necessary to conduct a CI investigation.

Mitigation: This risk is mitigated. Through the strict adherence to DHS I&A Instruction No. IA-1000,[69] DHS CI Program personnel have 180 days[70] from the date of collection of USPER data to determine whether the USPER data meets a two-part test: 1) is necessary for the conduct of an authorized national or departmental mission; and 2) collected information is reasonably believed to fall within one of I&A's authorized information categories. If the collected data does not meet the two-part test, the records are to be disposed of immediately, but no later than 180 days[71] from the date collected. If, however, the USPER data meet the two-part test, the records must be reviewed annually to determine whether there is still a mission need to retain the data. At the anniversary date (or any time beforehand) a record must be reviewed and verified to determine that a mission need remains that requires the data to be retained.

Section 6.0 Information Sharing

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 a CI 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)[72] to notify the FBI and provide access to any DHS records for investigative purposes. If other misconduct that raises law enforcement or other national security concerns is uncovered by the DHS CI Program, the misconduct is referred to the appropriate investigative agency at the federal, state, or local level. All information shared outside of DHS by the DHS CI Program will be on a memorandum with formal letterhead, as well as reviewed

[69] INSTRUCTION NO. IA-1000, *supra* note 10.
[70] USCG CI Program has 90 days currently and will have five years with the revised COMDTINST M3820.12.
[71] USCG CI Program will dispose of all USPER information within 90 days if it does not meet procedures to retain. Under the revised COMDTINST M3820.12, the USCG CI Program will dispose of all USPER information within five years if it does not meet procedures to retain.
[72] 50 U.S.C. § 3381(e).

and cleared for dissemination by the DHS CI Program. Any information shared with other federal agencies, state and local authorities, and the private sector will be in a manner consistent with the relevant routine use identified in the I&A ERS SORN,[73] as well as the forthcoming CI 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 DHS is compatible with the original collections listed in the SORNs for the source systems from which information is collected or pursuant to routine uses outlined in the forthcoming DHS/ALL-046 Counterintelligence Program System of Records, which will provide more sufficient notice of how DHS shares records from the unified Counterintelligence Program. Generally, information is shared for law enforcement, intelligence, and/or national security purposes and with contractors working for the federal government to accomplish agency functions related to the system of records.

DHS shares information only pursuant to routine uses outlined in the SORNs listed above or through business requirements, an approved memorandum of understanding (MOU), or approved information sharing agreement (ISA), such as the sharing described in Section 6.1. Any records created by DHS Components under the DHS CI Program remain under the centralized control of I&A. In addition, DHS re-disseminates information in accordance with the Privacy Act.

There are several routine uses from the ERS SORN that allow for the sharing of this information with other agencies consistent with this purpose, as described in this PIA:

Routine Use A states that information can be provided to any federal, state, local, tribal, territorial, foreign, or multinational government or agency, or appropriate private sector individuals and organizations, with responsibilities relating to homeland security, including responsibilities to counter, deter, prevent, prepare for, respond to, or recover from a natural or manmade threat, including an act of terrorism, or to assist in or facilitate the coordination of homeland security threat awareness, assessment, analysis, deterrence, prevention, preemption, and response.[74]

---

[73] For the USCG, the relevant routine uses are identified in the DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder, *supra* note 52.

[74] DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder Routine Use A provides a similar routine use, stating that information can be provided "To an appropriate federal, state, territorial, tribal, local, international, or foreign government intelligence entity, counterterrorism agency, or other appropriate authority charged with investigating threats or potential threats to national or international security or assisting in counterterrorism efforts, where a record, either on its face or in conjunction with other information, identifies a threat or potential threat to national or international security, or DHS reasonably believes the information may be useful in countering a threat or potential treat, which includes terrorist and espionage activities, and disclosure is appropriate to the proper performance of the official duties of the person receiving the disclosure."

Routine Use B states that data can be provided to a federal, state, local, tribal, territorial, foreign, or multinational government or agency with the responsibility and authority for investigating, prosecuting and/or enforcing a law (civil or criminal), regulation, rule, order or contract, where the record, on its face or in conjunction with other information, indicates a violation or potential violation of any such law, regulation, rule, order, or contract enforced by that government or agency.[75]

Routine Use C states that information can be provided data to a federal, state, local, tribal, territorial, foreign, or multinational government or agency, or other entity, including, as appropriate, certain private sector individuals and organizations, where disclosure is in furtherance of I&A's information sharing responsibilities under the Homeland Security Act of 2002, as amended, the Intelligence Reform and Terrorism Prevention Act of 2004, the National Security Act of 1947, as amended, Executive Order 12333, as amended, or any successor order, national security directive, intelligence community directive, other directive applicable to I&A, and any classified or unclassified implementing procedures promulgated pursuant to such orders and directives, or any other statute, Executive Order or directive of general applicability, and where such disclosure is otherwise compatible with the purpose for which the record was originally acquired or created by I&A.

Routine Use D states that data can be provided to federal, state, local, tribal, or territorial government or agency lawfully engaged in the collection of intelligence (including national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, law enforcement or law enforcement intelligence, and other information, where disclosure is undertaken for intelligence, counterterrorism, homeland security, or related law enforcement purposes, as authorized by U.S. Law or Executive Order, and in accordance with applicable disclosure policies.[76]

Routine Use E states that data can be provided to any other agency within the IC, as defined in section 3.4(f) of Executive Order 12333 of December 4, 1981, as amended, for the purpose of allowing that agency to determine whether the information is relevant and necessary to

[75] DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder Routine Use K provides a similar routine use, stating that information can be provided "To an appropriate federal, state, territorial, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure."

[76] DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder Routine Use B provides a similar routine use, stating that information can be provided "To a federal, state, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive."

its mission-related responsibilities and in accordance with that agency's classified or unclassified implementing procedures promulgated pursuant to such orders promulgated pursuant to such orders and directives, or any other statute, Executive Order or directive of general applicability.[77]

Routine Use G states that data can be provided to any individual, organization, or entity, as appropriate, to notify them of a serious threat to homeland security for the purpose of guarding them against or responding to such a threat, or where there is a reason to believe that the recipient is or could become the target of a particular threat, to the extent the information is relevant to the protection of life, health, or property.[78]

Routine Use Q states that data can be provided to an appropriate federal, state, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

6.3 Does the project place limitations on re-dissemination?

Recipients of information from the DHS CI Program must follow the "Third Agency Rule."[79] This rule mandates that prior to sharing data with a third agency (not involved in the original sharing agreement), the agency that intends to share will acquire consent from the agency that provided the data or information. If Components are granted access to DHS CI Program data, component analysts will be notified of this mandate, and will be required to follow this process as a condition of accessing DHS CI Program data. Only individuals with a need-to-know and a job-

[77] DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder Routine Use O provides a similar routine use, stating that information can be provided "To a federal, state, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence."

[78] DHS/USCG-062 Law Enforcement Information Database (LEIDB)/Pathfinder Routine Use I provides a similar routine use, stating that information can be provided "To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure."

[79] Executive Order 13526, 3 C.F.R. § 13526 (2009) at 4.1(i). The "Third Agency Rule" provides that "classified information originating in one agency may be disseminated to another agency or U.S. entity by any agency to which it has been made available without the consent of the originating agency, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information."

related requirement to have it will be able to gain access to DHS CI Program data.

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

The DHS CI Program's dissemination of information about USPERs is governed by DHS I&A Instruction No. IA-1000.[80] To further mitigate this risk, any DHS CI Program external disclosure of information must also meet additional restrictions pursuant to DHS Instruction No. 264-01-002, that requires the DHS CI Director's approval. The DHS CI Director's Staff 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.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that authorized users, who are exposed to PII as a routine part of their official duties, may make an inappropriate disclosure of information, either intentionally or unintentionally.

Mitigation: This risk is mitigated. Authorized users are required to complete annual specialized training on privacy and Intelligence Oversight, including the appropriate and inappropriate uses and disclosures of the information to all IC personnel. DHS CI Program personnel use of systems and access to data is monitored and audited. Should a user inappropriately disclose this information, he or she is subject to the loss of access, as well as disciplinary action up to and including the loss of a security clearance and/or termination. Depending on the circumstances, a user could also be liable for civil penalties under the Privacy Act or criminal penalties for violation of national security laws, with accompanying fines and/or imprisonment.

Privacy Risk: There is a privacy risk that information could be shared beyond the audience for whom it was originally intended.

Mitigation: This risk is mitigated. The DHS CI Program disseminates information about individuals in accordance with DHS I&A Instruction No. IA-1000.[81] To further mitigate this risk, any DHS CI Program external disclosure of information must also meet additional restrictions pursuant to DHS Instruction No. 264-01-002, that requires DHS CI Director approval. The DHS CI Director's Staff reviews 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. In addition, depending on the circumstances, a user could also be liable for civil penalties under the Privacy Act or criminal penalties for violation of national security laws, with accompanying fines and/or imprisonment.

[80] INSTRUCTION NO. IA-1000, *supra* note 10. The USCG CI Program's dissemination of information about USPER is governed by COMDTINST M3820.12.
[81] The USCG mitigates the risk through COMDTINST M3820.12.

Section 7.0 Redress

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

Because the DHS CI Program contains classified and sensitive but unclassified information related to intelligence; counter terrorism; homeland security; and law enforcement programs, activities, and investigations, records within it have been exempted from requests for access or amendment by covered individuals to their own information within it, to the extent permitted by the Privacy Act and subsection (k)(1), (k)(2), and (k)(5).[82]

Source systems SORNs describe the correction and redress process for source records. However, a traditional approach to individual participation is not practical for the DHS CI Program, whose mission is to protect DHS and the Homeland Security Enterprise from foreign and other adversarial threats. In keeping with this, and in accordance with Privacy Act requirements, DHS has exempted the I&A Enterprise Records System (ERS) from the Privacy Act's requirement to permit individuals access to records about themselves held by I&A and has published a final rule to amend its regulations to reflect this exemption.[83] Allowing an individual to access information held by the DHS CI Program could notify the individual that he or she is the focus of a counterintelligence investigation, which would permit the individual to impede the DHS CI Program efforts to protect homeland security; reveal sensitive methods or confidential sources used to acquire the relevant information; or implicate an ongoing law enforcement investigation and permit the individual to impede the investigation. DHS regulations establish and further justify this exemption.

Notwithstanding applicable exemptions, DHS reviews all requests for access, regardless of citizenship or immigration status, on a case-by-case basis. When such a request is made, and compliance 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. DHS has a process in place to provide an individual the opportunity to request access to his or her record(s) and request the correction of his or her record(s). DHS will review each request and may waive the exemption for access to records when it believes that providing access would not adversely affect homeland security efforts. Individuals seeking access to any record containing information that is part of an I&A system of records, or seeking to contest the accuracy of its content, may submit a Freedom

[82] 5 U.S.C. § 552a(k).
[83] Implementation of Exemptions; Office of Intelligence and Analysis Enterprise Records System, *supra* note 21. For the USCG LEIDB/PATHFINDER SORN, *see* Implementation of Exemptions; U.S. Coast Guard Law Enforcement Information Database (LEIDB)/Pathfinder, *supra* note 52.

of Information Act (FOIA) or Privacy Act request to DHS.[84] Given the nature of the sensitive law enforcement and intelligence information collected, DHS may not always permit the individual to gain access to or request amendment of his or her record. However, requests processed under the Privacy Act will also be processed under FOIA; requesters will always be given the benefit of the statute with the more liberal release requirements. FOIA does not grant an absolute right to examine government documents; it establishes the right to request records and to receive a response to the request. Instructions for filing a FOIA or Privacy Act request are available at www.dhs.gov/privacy.

Under the Information Sharing Environment (ISE) Privacy and Civil Liberties Protection Policy,[85] DHS established a process to permit individuals to file a privacy complaint. Individuals who have privacy complaints concerning analytic division intelligence activities may submit complaints to the Privacy Office at privacy@hq.dhs.gov. Individuals may also submit complaints alleging abuses of civil rights and civil liberties or possible violations of privacy protections by DHS employees, contractors, or grantees to the OIG at the OIG Hotline website.[86] Additionally, individuals may file complaints alleging violations of civil rights and civil liberties by going to the DHS Office of Civil Rights and Civil Liberties (CRCL) website,[87] completing the fillable form, and emailing it to CRCLCompliance@hq.dhs.gov.

The procedures for submitting FOIA requests for DHS CI Program records are available in 6 C.F.R. Part 5. FOIA requests can be submitted via mail or e-mail:

Office of Intelligence & Analysis
U.S. Department of Homeland Security
Washington, D.C. 20528
Attn: FOIA Officer
E-mail: I&AFOIA@hq.dhs.gov

[84] Individuals seeking access to USCG records may submit a FOIA or Privacy Act request to the USCG. *See* U.S. COAST GUARD, FREEDOM OF INFORMATION ACT, https://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-Engineering-Logistics-CG-4-/FOIA/ (last visited July 23, 2020).
[85] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, PRIVACY AND CIVIL LIBERTIES POLICY GUIDANCE MEMORANDUM, NO. 2009-01, THE DEPARTMENT OF HOMELAND SECURITY'S FEDERAL INFORMATION SHARING ENVIRONMENT PRIVACY AND CIVIL LIBERTIES PROTECTION POLICY (2009), *available at* https://www.dhs.gov/sites/default/files/publications/privacy_crcl_guidance_ise_2009-01_0.pdf.
[86] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF INSPECTOR GENERAL, HOTLINE: HOTLINE REPORT CORRUPTION, FRAUD, WASTE, ABUSE, MISMANAGEMENT, OR MISCONDUCT, *available at* https://www.oig.dhs.gov/hotline (last visited July 23, 2020).
[87] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF CIVIL RIGHTS AND CIVIL LIBERTIES, MAKE A CIVIL RIGHTS COMPLAINT, https://www.dhs.gov/file-civil-rights-complaint (last visited July 23, 2020).

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

As discussed in section 7.1, the ERS SORN (the LEIDB/Pathfinder SORN in the case of USCG), and the forthcoming CI SORN have been/will be exempted from the Privacy Act's requirements to permit individual access. Individuals may request access to their records under the FOIA process described above, and DHS may, on a selective basis, provide the requested records. Individuals may also file a privacy complaint as previously described.

If incorrect information is discovered within a published intelligence product, a revised version is published to correct the information or to note the questionable fact or content. Additionally, as previously noted under DHS I&A Instruction No. IA-1000, products containing USPER information are reviewed on an annual basis to determine whether continued retention of the information is necessary to the conduct of an authorized national or departmental mission.

As noted above, any requests from the public for information from the DHS CI Program will be reviewed on a case-by-case basis in light of the reasons the DHS CI Program is exempted from certain provisions of the Privacy Act.

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

Individuals are notified of the exemption to access and the justification for this exemption through this PIA, the ERS SORN (the LEIDB/Pathfinder SORN in the case of USCG), and the forthcoming CI SORN. Individuals are notified of the procedures for filing a FOIA request and filing a privacy complaint on the public DHS website at the links identified in question 7.1.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that individuals may not know that their information is being maintained by the DHS CI Program and therefore be unable to correct inaccurate information through the redress process.

Mitigation: This risk is partially mitigated. Though there is no way to provide notice to all of the individuals whose information is being held in the system, and the ability of a person to access and correct information held by the DHS CI Program is limited because of the sensitivity of the mission. DHS CI Program personnel are trained in analytic tradecraft to collaborate and apply expertise and logic to make the most accurate judgments and assessments possible given the information available.

All products containing USPER information are subject to DHS I&A Instruction No. IA-1000. The ISE Privacy and Civil Liberties Policy requires that analysts endeavor to use and share

information on USPERs that is reasonably considered accurate and appropriate for their documented purposes and to protect data integrity. This policy also requires analysts to notify others in the ISE when information that is determined to be inaccurate is disseminated or received by I&A.

In addition, individuals, regardless of immigration status, may request access to their records under FOIA. Additionally, U.S. Persons may request access under the Privacy Act. Individuals may also file a privacy complaint with the DHS Privacy Office, and a civil rights and civil liberties complaint with CRCL or the OIG.

Section 8.0 Auditing and Accountability

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

The DHS CI Program implements extensive auditing through the various applications that support the DHS CI Program. Although the specifics of these systems and applications are classified, CIIMS logs every action by DHS CI Program personnel. Audit logs are reviewed by the CIIMS system administrators, and DHS CI Program personnel are not able to access or modify the audit logs. Audit logs are maintained indefinitely, and should an incident occur, logs will be reviewed post-incident.

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

All personnel with DHS CI Program accounts are required to take annual privacy awareness training. Additionally, all DHS users are required to take information security awareness training annually. Users who fail to take Intelligence Oversight training within one year have their Top Secret/Sensitive Compartment Information (TS/SCI) network account suspended, and their account is not be reinstated until they complete the specified training.

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 DHS CI Program personnel who require access to the functionality and data in the DHS CI Program as a part of the performance of their official duties, and maintain appropriate clearances or permissions, have access to data. All DHS CI Program personnel are required to hold and maintain a TS/SCI clearance. DHS CI Program 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 DHS CI Program personnel. If issues are raised concerning DHS CI Program compliance with approved policies and procedures, the issues

will be immediately reviewed by the DHS CI Director and Staff. The DHS CI Director may conduct an audit or review and recommend remedial actions to the DCIX.

DHS maintains system access records showing which DHS CI Program personnel have accessed an automation system, which functions they have used, and which data they have accessed. DHS CI Program management revokes a user's access when no longer needed or permitted.

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 DHS CI Program information by organizations both internal and external to DHS are reviewed and approved by the DHS CI Director, as required by the DHS Instruction No. 264-01-002.

Responsible Officials

Robert Hale
DHS Counterintelligence Program
DHS I&A Counterintelligence Mission Center
(202) 282-9976

Lara Ballard
Privacy Officer
Office of Intelligence & Analysis
U.S. Department of Homeland Security

Tina Gabbrielli
DHS Counterintelligence Program Director
Office of Intelligence & Analysis
U.S. Department of Homeland Security

Kathleen Claffie
Chief, Office of Privacy Management (CG-6P)
United States Coast Guard
U.S. Department of Homeland Security

Approval Signature

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

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717

Appendix A: Counterintelligence Indicators

Indicators of Espionage	
Foreign influence or connections	• When not related to official duties, witting contact with persons known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against facilities, organizations, personnel, or information systems. This includes contact through social events or social networking sites. • Frequent or regular contact with foreign persons from countries that represent an intelligence or terrorist threat to the United States. • Visits to a foreign embassy, consulate, trade, or press office, either in the Continental United States (CONUS) or Outside the Continental United States (OCONUS), that are unexplained or inconsistent with an individual's official duties. • Contact with foreign government officials, including those who are known or suspected of being associated with a foreign intelligence or security organization, outside the scope of one's official duties. • Business connections, property ownership, or financial interests internal to a foreign country. • Sending large amounts of money to persons or financial institutions in foreign countries. • Receiving financial assistance from a foreign government, person, or organization.

Disregard for security practices	• Contact with any official or citizen of a foreign country when the foreign official or citizen:
	  ○ Exhibits excessive knowledge of or undue interest in personnel or their government duties beyond the normal scope of friendly conversation.
	  ○ Attempts to obtain classified or national security sensitive information.
	  ○ Attempts to place personnel under obligation through special treatment, favors, gifts, money, or other means.
	  ○ Attempts to establish business relationships that are improper or outside the scope of normal official duties.
	• Discussing classified information in unauthorized locations.
	• Improperly changing or removing security classification markings from documents and computer media.
	• Bringing unauthorized cameras, recording or transmission devices, laptops, modems, electronic storage media, cell phones, or software into areas where classified data is stored, discussed, or processed.
	• Repeated involvement in security violations, unwillingness to comply with rules and regulations, or unwillingness to comply with information security requirements.

	• Removing, downloading, or printing classified data from DHS computer systems beyond the normal scope of responsibilities. • Removing or sending classified or sensitive material out of secured areas without proper authorization. • Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.
Unusual work behavior	• Attempts to expand access to classified information by repeatedly volunteering for assignments or duties beyond the normal scope of responsibilities. • Attempts to obtain information for which the person has no authorized access or need-to-know. • Using copy, facsimile machines, document scanners, or other automated or digital equipment to reproduce or transmit classified material beyond the normal scope of responsibilities. • Repeatedly performing non-required work outside of normal duty hours, especially if unaccompanied. • Requesting extensions in one assignment or location when the assignment offers significant access to classified information (sometimes referred to as "Homesteading").
Financial matters	• Unexplained or undue affluence without a logical income source. Examples include: o Free spending or lavish display of wealth that appears beyond normal income. o A bad financial situation that suddenly reverses, opening several bank accounts containing substantial sums of money, or the repayment of large debts or loans. o Sudden purchases of high value items where no logical income source exists. o Attempts to explain wealth as an inheritance, gambling luck, or a successful business venture, without facts supporting the explanation.
Foreign travel	• Frequent or unexplained trips of short duration to foreign countries. • Travel that appears unusual or inconsistent with a person's interests or financial means. • Travel that is concealed or done under false pretense.
Undue interest	• Persistent questioning about the duties of coworkers and their access to classified information, technology, or information systems. • An attempt to befriend or recruit someone for the purpose of obtaining classified or unclassified information.
Soliciting others	• Offers of extra income from an outside venture to those with sensitive jobs or access. • Attempts to place personnel or contractors under obligation through special treatment, favors, gifts, or money.

	• Attempts to entice coworkers into criminal situations that could lead to blackmail or extortion. • Requests to obtain classified information to which the requestor is not authorized access.

Indicators of Potential Exploitation of DHS Information Systems by Foreign Intelligence Entities

- Permitting others to acquire unauthorized access to classified or sensitive information systems.
- Manipulating, exploiting, or hacking government computer systems or local networks to gain unauthorized access.
- Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of U.S. Government information.
- Unauthorized password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
- Use of another person's account credentials.
- Tampering with or introducing unauthorized elements into information systems.
- Unauthorized use of Universal Serial Bus (USB), removable media, or other transfer devices.
- Downloading or installing non-approved computer applications on government systems.
- Unauthorized e-mail traffic to foreign destinations.
- Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
- Unexplained storage of encrypted data.
- Unauthorized use of multiple user or administrator accounts.
- Social engineering, electronic elicitation, e-mail spoofing, or spear phishing.
- Introduction of malicious code or blended threats such as viruses, worms, Trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data ex-filtration.
- Use of unauthorized scripts to detect and move data and files.
- Unauthorized manipulation of information in paper or electronic files.
- Excessive probing or scanning from either an internal or external source.
- Rootkits, remote access tools, and other "backdoors."
- Exfiltration of data to unauthorized domains or cross domain violations.
- Unauthorized downloads or uploads of sensitive data.
- Unexplained or unauthorized data or software deletion.

- Log manipulation.
- Unauthorized use of intrusion detection systems.

Appendix B: Types of information collected by DHS CI Program

- Individuals who are known, reasonably believed to be, or are suspected of being, involved in or linked to:
    - The existence, organization, capabilities, plans, communications, intentions, and vulnerabilities of, means of finance or material support for, and activities against or threats to the United States or U.S. Persons and interests by, international terrorist groups or activities;
    - Groups or individuals believed to be assisting or associated with international terrorist groups or activities;
    - Activities undertaken by DHS personnel reasonably believed to be for the benefit of a foreign intelligence entity or agent thereof that constitutes a threat to homeland security, and/or activities that are preparatory to, or which facilitate or support such activities, including:
        - Activities related to the violation or suspected violation of immigration or customs laws and regulations of the United States;
        - Activities, which could reasonably be expected to assist in the development or use of a weapon of mass effect;
        - Activities to identify, create, exploit, or undermine the vulnerabilities of the "key resources" (as defined in section 2(9) of the Homeland Security Act of 2002) and "critical infrastructure" (as defined in 42 U.S.C. § 5195c(c)) of the United States;
        - Activities to identify, create, exploit, or undermine the vulnerabilities of the cyber and national telecommunications infrastructure, including activities which may impact the availability of a viable national security and emergency preparedness communications infrastructure;
        - Activities detrimental to the security of transportation and transportation systems;
        - Activities which violate or are suspected of violating the laws relating to counterfeiting of obligations and securities of the United States and other financial crimes, including access device fraud, financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure;

- Activities, not wholly conducted within the United States, which violate or are suspected of violating the laws which prohibit the production, transfer, or sale of narcotics or substances controlled in accordance with Title 21 of the United States Code, or those associated activities otherwise prohibited by Titles 21 and 46 of the United States Code;
- Activities which impact or concern the security, safety, and integrity of our international borders, including any illegal activities that cross our borders such as violations of the immigration or customs laws of the United States;
- Activities which impact, concern, or otherwise threaten the safety and security of the President and Vice President, their families, heads of state, and other designated individuals; the White House, Vice President's residence, foreign missions, and other designated buildings within the United States;
- Activities which impact, concern, or otherwise threaten maritime safety and security, maritime mobility and navigation, or the integrity of the maritime environment;
- Activities which impact, concern, or otherwise threaten the national operational capability of the Department to respond to natural and man-made major disasters and emergencies, including acts of terrorism, in support of impacted communities; to coordinate all federal emergency management response operations, response planning and logistics programs; and to integrate federal, state, tribal and local response programs to ensure the efficient and effective delivery of immediate emergency assistance to individuals and communities impacted by major disasters, emergencies or acts of terrorism; and
- Activities involving the detection of and response to unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the United States.

- The capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, where the individuals may be officers or employees of, or otherwise acting for or on behalf of, a foreign power or organization that may be owned or controlled, directly or indirectly, by a foreign power;
- Intelligence activities, or other individuals known or suspected of engaging in intelligence activities, on behalf of a foreign power or terrorist group:

- Individuals who voluntarily request assistance or information, through any means, from I&A, or individuals who voluntarily provide information concerning any of the activities above, which may threaten or otherwise affect homeland security.

- Information collected and stored by the DHS CI Program from the above listed categories includes:
  - Classified and unclassified intelligence (includes national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, and related law enforcement information, including source records and the reporting and results of any analysis of this information, obtained from all agencies, components and organizations of the federal government, including the IC; foreign governments, organizations or entities, and international organizations; state, local, tribal and territorial government agencies (including law enforcement agencies); and private sector entities;
  - Information provided by record subjects and individual members of the public;
  - Information obtained from the Terrorist Screening Center, the National Counterterrorism Center, or from other organizations about individuals known or reasonably suspected of being engaged in conduct constituting, preparing for, aiding, or relating to terrorism;
  - Active and historical law enforcement investigative information;
  - Information related to lawful DHS Security investigations, including authorized physical, personnel, and communications security investigations, and information systems security analysis and reporting;
  - Operational and administrative records, including correspondence records;
  - Lawfully acquired financial information, when relevant to an authorized intelligence, counterterrorism, homeland security, or related law enforcement activity;
  - Public source data such as that contained in media, including periodicals, newspapers, broadcast transcripts, and other public reports and commercial databases; and
  - Data about the providers of any information otherwise contained within this system, including the means of transmission of the data.

- These records consist of identifying data, including:

- Individual's name and aliases; Physical description; Citizenship; Biometrics; Date and Place of birth; Social Security number; Security clearance information; Telephone and cell phone numbers; Physical and mailing addresses; Electronic mail addresses; Vehicular information; Photographs; Education; Medical history; Travel history including passport information; Financial data; Criminal history; Work experience; Relatives and associates.
- Investigative files containing allegations and complaints; witness statements; transcripts of electronic monitoring; subpoenas and legal opinions and advice; reports of investigation; reports of criminal, civil, and administrative actions taken as a result of the investigation; and other relevant evidence; handwriting exemplars; laboratory analyses of inks and papers; handwriting analyses; information, reports or opinions from the forensic examination of documentary and digital media evidence; polygraph case files; search warrants and search warrant returns; indictments; certified inventories of property held as evidence; sworn and unsworn witness statements; state, local, and foreign criminal investigative information and reports; names and telephone numbers of persons intercepted by electronic, mechanical, or other device under the provisions of 18 U.S.C. § 2510, et seq, compiled during the lawful course of a criminal or civil investigation.
- Any other personal information relevant to the subject matter of a DHS counterintelligence investigation.