



Department of Homeland Security

2018 Privacy Office Annual Report to Congress

For the period July 1, 2017 – June 30, 2018

October 10, 2018



Homeland
Security

Message from the Chief Privacy Officer

October 10, 2018

I am pleased to present the Department of Homeland Security Privacy Office's *2018 Annual Report to Congress*, highlighting the achievements of the Privacy Office from July 2017 through June 2018.



The Privacy Office had another productive and busy year, working closely with privacy professionals and operational Components throughout the Department on priority initiatives, including:

- Screening and vetting initiatives: The Privacy Office continued playing a key role in the identification and mitigation of potential privacy risks associated with the Department's implementation of Executive Order 13780, "*Protecting the Nation from Foreign Terrorist Entry into the United States*," as well as with other Departmental initiatives associated with the screening and vetting mission.
- Violence Against Women Act: Congress provided the Privacy Office with additional funding this year to ensure information and data released by the Department does not reveal the identity or personal information of non-U.S. Persons who may be survivors of domestic violence, sexual assault, stalking, human trafficking, or other crimes. The Privacy Office and the Office for Civil Rights and Civil Liberties (CRCL) developed a process for the two offices to share incidents of unauthorized disclosures, and partner to investigate and mitigate these incidents.
- Breach response and mitigation: As part of the updated *DHS Instruction Guide 047-01-008, Privacy Incident Handling Guidance*, the Chief Privacy Officer now has the authority and ability to convene and lead a Breach Response Team when a "major incident" involving Personally Identifiable Information (PII) has occurred, or when the Chief Privacy Officer has determined the potential impact of a privacy incident is significant enough to warrant a more fulsome response. To promote the Instruction and educate our partners, the Privacy Office hosted the first Annual DHS Privacy Incident Tabletop Exercise to examine the key decisions required to mitigate a privacy incident, as well as the roles and responsibilities outlined in the Department's breach response plan.

Priorities that will take us into the new fiscal year include:

- Reducing the collection and use of Social Security numbers (SSN): The Privacy Office is currently finalizing a policy that will require system owners to use an alternative personal identifier in place of the SSN, or to mask or truncate the SSN wherever it appears.
- Preventing terrorism through biometrics: The Privacy Office is working closely with U.S. Customs and Border Protection (CBP) to ensure that facial recognition technology used to verify a traveler's identity is implemented in a privacy-protective manner, as required by federal mandates.

-
- *Streamlining Freedom of Information Act Information Technology*: The Privacy Office and the Office of the Chief Information Officer (CIO) have formed an enterprise-wide FOIA IT System Working Group to create functional requirements for a new streamlined FOIA processing and case management system that will save money, provide more consistent and accurate reporting on DHS programs and activities, satisfy statutory requirements for DHS to receive FOIA requests electronically through FOIA.gov, and allow DHS to move from paper-based to electronic processes.

The Privacy Office will begin a new fiscal year in October with a new Strategic Plan to take us through the next four years. The new plan will align with the Secretary's vision for the Department, while taking into account the fiscal environment in which we will be operating for the near future.

To position the Privacy Office for success in implementing the new plan, I have two expectations. First, our revised goals and objectives must be ambitious, but achievable. Second, in order to promote ownership and meaningful assessment of our progress, our goals and objectives must be measurable. This will enable the Privacy Office leadership team to engage productively with the DHS privacy enterprise and operational professionals throughout the agency on solutions, as well as to cascade our Strategic Plan into workforce development opportunities and expectations for individual employee performance.

Please direct any inquiries about this report to the Office of Legislative Affairs at 202-447-5890 or privacy@dhs.gov.

Sincerely,



Philip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security

Pursuant to congressional notification requirements, this report is being provided to the following Members of Congress:

The Honorable Ron Johnson

Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Claire McCaskill

Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Charles Grassley

Chairman, U.S. Senate Committee on the Judiciary

The Honorable Dianne Feinstein

Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Richard Burr

Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Mark Warner

Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Michael McCaul

Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson

Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Trey Gowdy

Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings

Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Bob Goodlatte

Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable Jerry Nadler

Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Devin Nunes

Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Adam Schiff

Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

Executive Summary

The work of the DHS Privacy Office supports all five core DHS missions articulated in the 2014 [Quadrennial Homeland Security Review](#): (1) prevent terrorism and enhance security; (2) secure our borders; (3) enforce our immigration laws; (4) safeguard cyberspace; and (5) strengthen national preparedness, as well as the important cross-cutting goal to *mature and strengthen homeland security by integrating information sharing and preserving privacy, oversight, and transparency in the execution of all departmental activities*. In addition, through training, outreach, and participation in departmental program development, the Privacy Office advances the guiding principles and core values outlined in the [DHS Strategic Plan for Fiscal Years 2014-2018](#).



To accomplish these key outcomes, the Privacy Office established four goals in its [Fiscal Year 2015-2018 Strategic Plan](#), each supported by specific and measurable objectives, and explained in detail in the chapters that follow:

- **Goal 1 (Privacy and Disclosure Policy):** Foster a culture of privacy and disclosure and demonstrate leadership through policy and partnerships;
- **Goal 2 (Outreach, Education, and Reporting):** Provide outreach, education, training, and reports in order to promote privacy and transparency in homeland security;
- **Goal 3 (Compliance and Oversight):** Conduct robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all DHS activities, and promote privacy best practices and guidance to the Department's information sharing and intelligence activities; and
- **Goal 4 (Workforce Excellence):** Develop and retain the best privacy and disclosure professionals in the Federal Government.

Key Privacy Office achievements during the reporting period¹ are listed below under the related strategic goal. More details on each of these items, and additional achievements, can be found in the body of the report.

Goal 1: Privacy and Disclosure Policy

- Issued the following privacy policy documents related to privacy incidents in response to Office of Management and Budget (OMB) guidance issued in January 2017, [Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information \(PII\)](#):

¹ The reporting period is June 30 of the prior year through July 1 of this year, but we also include significant accomplishments finalized after July 1 and up to the publication date of the report.

-
- **New:** [*Privacy Incident Responsibilities and Breach Response Team*](#), establishes the requirement for the Chief Privacy Officer to convene and lead a Breach Response Team when a “major incident” that includes PII has occurred, or at the discretion of the Chief Privacy Officer.
 - **Revised:** [*Privacy Incident Handling Guidance*](#) (PIHG) establishes DHS policy for responding to privacy incidents by providing procedures to follow upon the detection or discovery of a suspected or confirmed incident involving PII in an unclassified environment.
 - **Revised:** [*Handbook for Safeguarding Sensitive PII*](#) provides best practices and policy requirements to prevent a privacy incident involving Sensitive PII during all stages of the information lifecycle: *when collecting, storing, using, disseminating, or disposing of Sensitive PII*
 - Issued [*Instruction 262-11-001, Freedom of Information Act Compliance on Employee Notification*](#) to formalize an employee notification process to inform current Department employees when their employment records, as defined in the instruction, are about to be released under the FOIA.
 - *Screening and vetting initiatives:* The Privacy Office began participating in several intra- and inter-agency working groups and meetings to identify and mitigate privacy concerns that may arise from implementation of Executive Order 13780, “*Protecting the Nation from Foreign Terrorist Entry into the United States,*” and other recent proposals for enhanced screening and vetting measures. Two such initiatives are related to the implementation activities associated with National Security Presidential Memoranda (NSPM) -7 and NSPM-9.
 - In the FY 2018 *Appropriations Act* for DHS, Congress provided the Privacy Office with additional funding to ensure information and data released by the Department does not reveal the identity or PII of non-U.S. Persons who may be survivors of domestic violence, sexual assault, stalking, human trafficking, or other crimes. The Privacy Office and the Office for Civil Rights and Civil Liberties (CRCL) developed a process for the two offices to share incidents of unauthorized disclosures, and partner to ensure that incidents are appropriately reviewed, investigated, addressed, and resolved.

Goal 2: Outreach, Education, and Reporting

- Hosted several informational meetings with members of the privacy advocacy community to inform them of key privacy initiatives throughout the year, including facial recognition and cybersecurity.
- Published the inaugural report to Congress required by the *Social Security Number Fraud Prevention Act of 2017*² to document the Privacy Office’s multi-year plan to reduce the collection, use, and mailing of Social Security numbers at DHS.

² Pub. L. No. 115-59, 131 Stat. 1152 (2017).

Goal 3: Compliance and Oversight

- Approved 69 new or updated Privacy Impact Assessments and 14 System of Records Notices, resulting in a Department-wide Federal Information Security Modernization Act privacy score of 97 percent for required investment technology system Privacy Impact Assessments, and 100 percent for System of Records Notices.
- Completed three and continued to work on one Privacy Compliance Review (PCR), oversaw implementation of recommendations from six previous PCRs, and launched one new PCR.
- Hosted, in conjunction with FEMA's National Exercise Division, the first Annual DHS Privacy Incident Tabletop Exercise in Washington, DC, with privacy representatives from all DHS Components in attendance. The tabletop exercise examined 1) key DHS decisions required to address a privacy incident; and 2) roles and responsibilities as outlined in the Privacy Incident Handling Guidance (PIHG).
- Decreased the FY 2017 FOIA backlog by six percent, from 46,788 requests in FY 2016 to 44,117 requests, owing to the concerted effort of the Privacy Office and our partner Components to address the Department's backlog.
- Reviewed 294 raw intelligence information reports (IIR) and draft intelligence reports (FINTEL), 35 briefing packages, and 347 Requests for Information (at all levels of classification). The Privacy Office's product review function is an ongoing, real-time operational service for the Department, requiring around-the-clock monitoring of communications and quick response to the Office of Intelligence and Analysis' requests for review of intelligence products.

Goal 4: Workforce Excellence

- Implemented several cost savings initiatives: leveraged intra-agency agreements with Departmental offices and Components to reimburse the Privacy Office for infrastructure and license costs related to FOIAXpress, the web-based, commercial-off-the-shelf application used for processing FOIA and Privacy Act requests; collected almost \$472,400 in reimbursable funding, directing more resources toward privacy and FOIA support services contracts; and conducted a review of IT billing, data management, and support requirements, resulting in an annual cost savings of \$245,000 for the Department.
- Hosted multiple workshops and training events to support the DHS Leadership Year, a year-long campaign highlighting the important principles and values that define effective leadership. The Chief Privacy Officer sponsored several events, including a recognition ceremony for disclosure professionals with the Deputy Secretary; a career-shadowing event with students from George Mason University; and a panel discussion with former Chief Privacy Officers that was attended by representatives from more than a dozen DHS Components.



Privacy Office

2018 Annual Report to Congress

Table of Contents

Message from the Chief Privacy Officer	i
Executive Summary.....	1
Table of Contents.....	4
Authorities and Responsibilities of the Chief Privacy Officer	6
Privacy Office Overview	9
I. Privacy and Disclosure Policy	14
Privacy Policy Leadership	16
II. Outreach, Education, and Reporting.....	26
Outreach.....	27
Education: Privacy & FOIA Training and Awareness.....	32
Reporting.....	35
III. Compliance & Oversight.....	36
Privacy Compliance.....	37
Information Sharing and Intelligence Activities	56
Privacy Incident Response.....	59
Privacy Complaints.....	64
IV. Workforce Excellence	68
V. Component Privacy Programs.....	70
Federal Emergency Management Agency (FEMA)	71

National Protection and Programs Directorate (NPPD).....	73
Office of Intelligence and Analysis (I&A).....	76
Transportation Security Administration (TSA).....	77
United States Citizenship and Immigration Services (USCIS)	79
United States Coast Guard (USCG).....	81
U.S. Customs and Border Protection (CBP)	83
United States Immigration and Customs Enforcement (ICE)	85
United States Secret Service (USSS or Secret Service).....	88
Appendix A – Acronyms	90
Appendix B – DHS Implementation of the Fair Information Practice Principles (FIPPs)....	93
Appendix C – Compliance Activities	94
Appendix D – Published PIAs and SORNs.....	97

Authorities and Responsibilities of the Chief Privacy Officer

Major Federal Privacy Laws

The Privacy Office accomplishes its mission through the framework of several federal privacy and transparency laws, including the following:

- *Privacy Act of 1974*, as amended (5 U.S.C. § 552a): Embodies a code of fair information principles that governs the collection, maintenance, use, and dissemination of personally identifiable information by federal agencies;
- *E-government Act of 2002* (Public Law 107-347): Mandates Privacy Impact Assessments (PIA) for all federal agencies when there are new collections of, or new technologies applied to, personally identifiable information;
- *Freedom of Information Act of 1966* (FOIA), as amended (5 U.S.C. § 552): Implements the principles that persons have a fundamental right to know what their government is doing; and
- *Implementing the Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53): Amends the Homeland Security Act to give new authorities to the Chief Privacy Officer (CPO).

Chief Privacy Officer's Statutory Authorities

The responsibilities of the CPO are set forth in Section 222 of the *Homeland Security Act of 2002*, as amended:

SEC. 222. [6 U.S.C. 142] PRIVACY OFFICER.

(a) APPOINTMENT AND RESPONSIBILITIES.—The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including—

- (1) assuring that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;
- (2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
- (3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
- (4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;
- (5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—
 - (A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and
 - (B) Congress receives appropriate reports on such programs, policies, and procedures; and
- (6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.

(b) AUTHORITY TO INVESTIGATE.—

-
- (1) **IN GENERAL.**—The senior official appointed under subsection (a) may—
- (A) have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the senior official under this section;
 - (B) make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official’s judgment, necessary or desirable;
 - (C) subject to the approval of the Secretary, require by subpoena the production, by any person other than a Federal agency, of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to performance of the responsibilities of the senior official under this section; and
 - (D) administer to or take from any person an oath, affirmation, or affidavit, whenever necessary to performance of the responsibilities of the senior official under this section. 7 “
- (2) **ENFORCEMENT OF SUBPOENAS.**—Any subpoena issued under paragraph (1)(C) shall, in the case of contumacy or refusal to obey, be enforceable by order of any appropriate United States district court.
- (3) **EFFECT OF OATHS.**—Any oath, affirmation, or affidavit administered or taken under paragraph (1)(D) by or before an employee of the Privacy Office designated for that purpose by the senior official appointed under subsection (a) shall have the same force and effect as if administered or taken by or before an officer having a seal of office.
- (c) **SUPERVISION AND COORDINATION.**—
- (1) **IN GENERAL.**—The senior official appointed under subsection (a) shall—
- (A) report to, and be under the general supervision of, the Secretary; and
 - (B) coordinate activities with the Inspector General of the Department in order to avoid duplication of effort.
- (2) **COORDINATION WITH THE INSPECTOR GENERAL.**—
- (A) **IN GENERAL.**—Except as provided in subparagraph (B), the senior official appointed under subsection (a) may investigate any matter relating to possible violations or abuse concerning the administration of any program or operation of the Department relevant to the purposes under this section.
- (B) **COORDINATION.**—
- (i) **REFERRAL.**—Before initiating any investigation described under subparagraph (A), the senior official shall refer the matter and all related complaints, allegations, and information to the Inspector General of the Department.
 - (ii) **DETERMINATIONS AND NOTIFICATIONS BY THE INSPECTOR GENERAL.**—
 - (I) **IN GENERAL.**—Not later than 30 days after the receipt of a matter referred under clause (i), the Inspector General shall—
 - (aa) make a determination regarding whether the Inspector General intends to initiate an audit or investigation of the matter referred under clause (i); and
 - (bb) notify the senior official of that determination.
 - (II) **INVESTIGATION NOT INITIATED.**—If the Inspector General notifies the senior official under sub clause (I)(bb) that the Inspector General intended to initiate an audit or investigation, but does not initiate that audit or investigation within 90 days after providing that notification, the Inspector General shall further notify the senior official that an audit or investigation was not initiated. The further notification under this sub clause shall be made not later than 3 days after the end of that 90-day period.

(iii) **INVESTIGATION BY SENIOR OFFICIAL.**—The senior official may investigate a matter referred under clause if—

(I) the Inspector General notifies the senior official under clause (ii)(I)(bb) that the Inspector General does not intend to initiate an audit or investigation relating to that matter; or

(II) the Inspector General provides a further notification under clause (ii)(II) relating to that matter.

(iv) **PRIVACY TRAINING.**—Any employee of the Office of Inspector General who audits or investigates any matter referred under clause (i) shall be required to receive adequate training on privacy laws, rules, and regulations, to be provided by an entity approved by the Inspector General in consultation with the senior official appointed under subsection (a).

(d) **NOTIFICATION TO CONGRESS ON REMOVAL.**— If the Secretary removes the senior official appointed under subsection (a) or transfers that senior official to another position or location within the Department, the Secretary shall—

(1) promptly submit a written notification of the removal or transfer to Houses of Congress; and

(2) include in any such notification the reasons for the removal or transfer.

(e) **REPORTS BY SENIOR OFFICIAL TO CONGRESS.**—The senior official appointed under subsection (a) shall—

(1) submit reports directly to the Congress regarding performance of the responsibilities of the senior official under this section, without any prior comment or amendment by the Secretary, Deputy Secretary, or any other officer or employee of the Department or the Office of Management and Budget; and

(2) inform the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives not later than—

(A) 30 days after the Secretary disapproves the senior official’s request for a subpoena under subsection (b)(1)(C) or the Secretary substantively modifies the requested subpoena; or

(B) 45 days after the senior official’s request for a subpoena under subsection (b)(1)(C), if that subpoena has not either been approved or disapproved by the Secretary.

Privacy Office Overview

The DHS Privacy Office (Privacy Office) is the first statutorily created privacy office in the Federal Government. The head of this office, the Chief Privacy Officer (CPO), reports directly to the Secretary of the Department, and the Privacy Office's mission and authority are founded upon the responsibilities set forth in section 222 of the *Homeland Security Act of 2002*, as amended.

The Privacy Office's mission is to protect individuals by embedding and enforcing privacy protections and transparency in all DHS activities.³ All DHS systems, technology, forms, and programs that either collect PII or have a privacy impact are subject to the oversight of the CPO and the requirements of U.S. data privacy and disclosure laws.

Privacy Office expertise in privacy and disclosure law help to inform privacy and disclosure policy development both within the Department and in collaboration with the rest of the Federal Government. The Privacy Office is responsible for evaluating Department programs, systems, and initiatives for potential privacy impacts, and providing mitigation strategies to reduce the privacy impact. The Privacy Office also advises senior leadership to ensure that privacy protections are implemented throughout the Department.

The Privacy Office helps to build a culture of privacy across the Department by training Department personnel on the importance of safeguarding privacy, and complying with federal laws and privacy policies.

Who We Serve

We serve the Department, other federal agencies, the American people, and immigrants and visitors to the United States.

What We Do

The Privacy Office works with every Component and program in the Department to ensure that privacy considerations are addressed when *planning or updating* any program, system, form, or initiative that may use PII. We work to ensure that technologies used at the Department sustain, and do not erode, privacy protections. We also implement the Department's Fair Information



³ Source: DHS Privacy Office FY 2015-2018 Strategic Plan. See hyperlink on page 11.

Practice Principles (FIPPs) governing the use of PII through a comprehensive compliance process.

The Privacy Office also:

- Evaluates Department legislative and regulatory proposals involving the collection, use, and disclosure of PII;
- Centralizes programmatic oversight of FOIA and Privacy Act operations and supports implementation across the Department;
- Operates a Department-wide Privacy Incident Response Program to ensure that incidents involving PII are properly reported, investigated, and mitigated, as appropriate;
- Responds to complaints of privacy violations and provides redress, as appropriate; and
- Provides training, education, and outreach to build a culture of privacy across the Department and transparency to the public.

The Fair Information Practice Principles (FIPP)

The FIPPs,⁴ shown in Figure 1, are the cornerstone of DHS's efforts to integrate privacy and transparency into all Department operations, in tandem with [DHS Privacy Policy 2017-01 Regarding the Collection, Use, Retention, and Dissemination of Personally Identifiable Information](#).

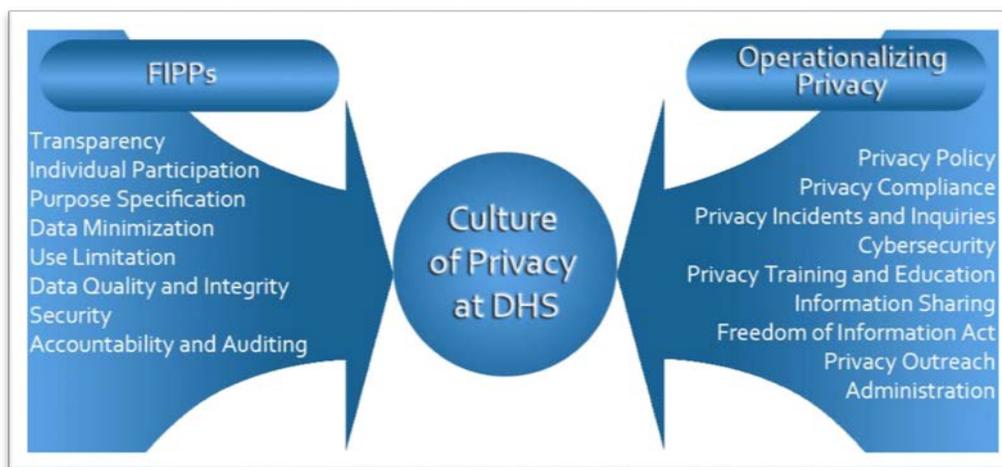


Figure 1: Privacy Office Implementation of the FIPPs

The Privacy Office incorporates these well-recognized principles into privacy and disclosure policy and compliance processes throughout the Department. We also undertake these statutory

⁴ The FIPPs are rooted in the Privacy Act of 1974, 5 U.S.C. § 552a, and memorialized in Privacy Policy Guidance Memorandum No. 2008-01 (re-designated as DHS Policy Directive 140-06), *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, (Dec. 29, 2008) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf, and in DHS Management Directive 047-01, *Privacy Policy and Compliance*, July 2011, available at <https://www.dhs.gov/publication/privacy-policy-and-compliance-directive-047-01>

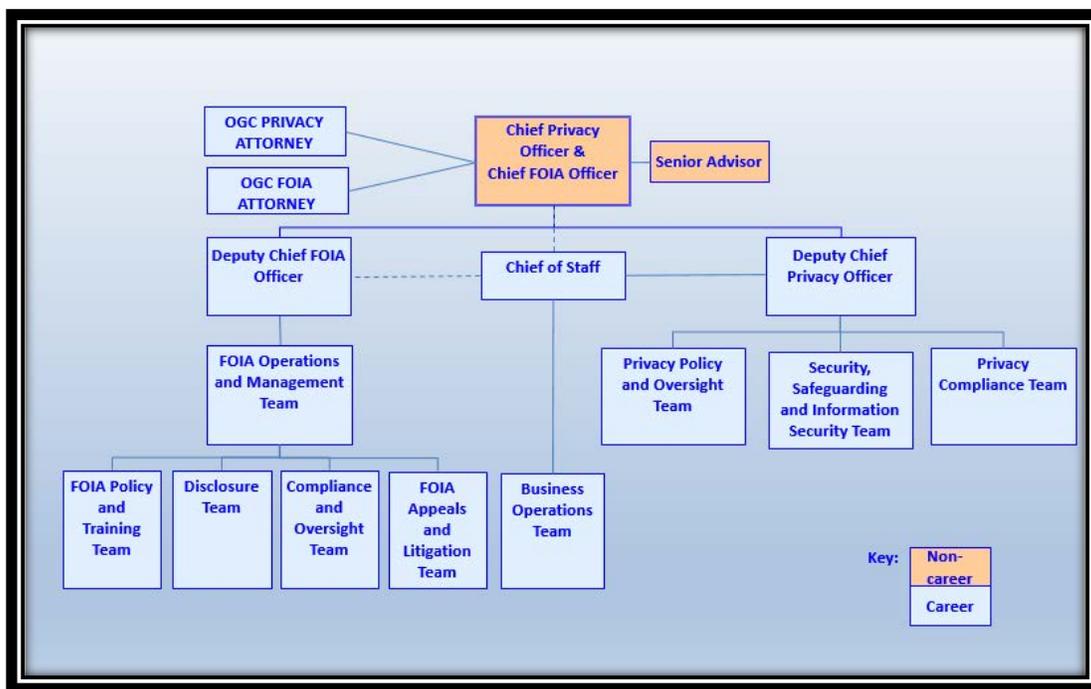
and policy-based responsibilities in collaboration with Component privacy officers,⁵ privacy points of contact (PPOC),⁶ Component FOIA Officers, and program offices to ensure that all privacy and disclosure issues are afforded the appropriate level of review and expertise.

Please refer to Appendix B for a detailed explanation of the FIPPs.

Privacy Office Structure

The organizational structure of the Privacy Office is aligned with, and accountable for, its four strategic goals as described in the [Privacy Office Fiscal Year \(FY\) 2015-2018 Strategic Plan](#). Figure 2 depicts the organizational structure of the Privacy Office.

Figure 2: Privacy Office Organizational Chart



The Privacy Office is composed of five teams:

- 1) The Privacy Policy and Oversight Team bears primary responsibility for developing DHS privacy policy, as well as providing subject matter expertise and support for policy development throughout the Department in areas that impact individual privacy. These areas include social media, “big data,” enterprise data management, cybersecurity, acquisitions and procurement, and international engagement. In addition, this team is dedicated to

⁵ Every DHS Component is required by DHS policy to appoint a Privacy Officer to oversee privacy compliance, policy, and oversight activities in coordination with the CPO. See [DHS Privacy Policy Instruction 047-01-005, Component Privacy Officer](#).

⁶ PPOCs are assigned responsibility for privacy within their respective components, directorates, or programs, but they are not generally full-time privacy officers. Their privacy-related duties may be in addition to their primary responsibilities. Like Component Privacy Officers, PPOCs work closely with component program managers and the Privacy Office to manage privacy matters within DHS.

implementing accountability and continually improving DHS privacy processes and programs, such as in the development of the National Vetting Center (NVC), established by National Security Presidential Memorandum - 9. This team also conducts Privacy Compliance Reviews (PCR) and privacy investigations, manages the Department's privacy incident response efforts, and oversees the Department's handling of privacy complaints. Finally, this team supports the privacy training, public outreach, and reporting functions of the Privacy Office.

- 2) The Privacy Compliance Team oversees privacy compliance activities, including supporting DHS Component privacy officers, PPOCs, and DHS programs. Examples of compliance activities include the review of Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), System of Records Notices (SORN), and other compliance documents. A brief description of the privacy compliance process can be found in Appendix C.
- 3) The Information Sharing, Safeguarding, and Security Team provides specialized privacy expertise to support DHS information-sharing initiatives with the U.S. Intelligence Community⁷ and federal, state, local, tribal, territorial, and international immigration and law enforcement partners. The team engages with operational, policy, and oversight stakeholders—both within DHS and with other federal partners—throughout the information sharing lifecycle by evaluating information sharing requests, assessing and mitigating privacy risks, and reviewing compliance with internal policies and agreement privacy terms and conditions. Team members participate in Privacy Office efforts to review intelligence products and Component-implemented intelligence rules, provide intelligence-related privacy training, and provide policy guidance for other related DHS initiatives, including but not limited to: safeguarding information and preventing insider threats, countering violent extremism, the sharing of biometric data both domestically and internationally, and the deployment of unmanned aircraft systems. The team also ensures DHS compliance with the *Computer Matching and Privacy Protection Act of 1988*.
- 4) The FOIA Team provides programmatic oversight of Department-wide FOIA operations and policy. The team comprises four groups: Disclosure; Policy and Training; Compliance and Oversight; and FOIA Appeals and Litigation. The Privacy Office is responsible for coordinating and overseeing the Components' FOIA operations, providing FOIA-related training, and preparing the required annual reports on the Department's FOIA performance. Through its FOIA team, the Privacy Office also processes initial FOIA and Privacy Act requests to the Office of the Secretary (including the Military Advisor's Office), and many offices within DHS Headquarters.⁸ The Privacy Office also reviews and analyzes appeals

⁷ A succinct definition is available on: www.dni.gov.

⁸ In this report, a reference to the "Department" or "DHS" means the entire Department of Homeland Security, including its Components, Directorates, and the Office of the Secretary. The DHS FOIA Office processes the Privacy Office's initial requests and those for the following offices: Office of the Secretary, Military Advisor's Office, Office of the Citizenship and Immigration Services Ombudsman, Office of the Executive Secretary, Office of Partnership and Engagement, Management Directorate, Office for Civil Rights and Civil Liberties, Office of Operations Coordination, Office of Strategy, Policy, and Plans, Office of the General Counsel, Office of Legislative Affairs, and Office of Public Affairs. In December 2017, DHS established the Countering Weapons of Mass

from denials of access to records requested under FOIA, recommends final agency decisions on the release/non-release of records, and assists the Office of the General Counsel (OGC) in the litigation process.

- 5) The Privacy Administrative Coordination Team (PACT) is the focal point for all administrative matters and works diligently to ensure efficiency of operations, including recruiting and maintaining a superior workforce of talented subject-matters experts. In addition to providing administrative support for all Privacy Office functions, PACT also manages resources, planning, official correspondence, workforce policy, staff development, resilience, facilities, and other infrastructure.

Working with the Privacy Office

Department personnel responsibilities:

- Partner with us when planning or updating any program, system, form, information sharing agreement, or initiative to ensure compliance with privacy law and policy;
- Know when to prepare privacy compliance documents;
- Promptly report privacy incidents;
- Educate yourself through Departmental Privacy and Disclosure Directives, Instructions, and Policy Guidance and our training programs on the proper handling of PII; and
- Respond promptly to all requests from FOIA professionals, and from privacy professionals reviewing programs and investigating incidents.

Privacy community and the public opportunities:

- Contact us so we can respond to your privacy concerns or questions;
- Contact the DHS FOIA Public Liaison for questions or concerns involving FOIA; and
- Participate in our workshops and educational opportunities.

International partner opportunities:

- Learn about the U.S. privacy framework and how DHS protects privacy;
- Work with us to create privacy-protective international information sharing agreements; and
- Help identify practical implementation mechanisms for established privacy best practices, such as the internationally-recognized Fair Information Practice Principles.

Destruction Office (CWMD), and consolidated the Domestic Nuclear Detection Office (DNDO) and a majority of the Office of Health Affairs, as well as other DHS functions, into CWMD.



I. Privacy and Disclosure Policy

The Privacy Office's FY 2015-2018 Strategic Plan includes four strategic goals:

Goal One (Privacy and Disclosure Policy): Foster a culture of privacy and disclosure and demonstrate leadership through policy and partnerships.

This section highlights the Privacy Office's development and support of new and ongoing policy initiatives to promote privacy and transparency at DHS during the reporting period.

The CPO has primary authority for privacy policy at the Department, as defined by [Privacy Policy and Compliance Directive 047-01](#). All Department personnel, including federal employees, independent consultants, and government contractors involved in Department programs must comply with DHS privacy policies.

The Privacy Office works to ensure that the use of technology sustains, and does not erode, privacy protections relating to the collection, use, dissemination, and maintenance of PII. We also provide subject matter expertise and support for policy development throughout the

Department in areas that impact individual privacy. These areas include big data, enterprise data management, cybersecurity, acquisitions and procurement, and intelligence products.

All DHS privacy policies are available on our website at: <https://www.dhs.gov/policy>

New or Revised Privacy Policies

In response to Office of Management and Budget (OMB) guidance issued in January 2017, *Memorandum M-17-12, Preparing for and Responding to a Breach of PII*, the Privacy Office issued one new privacy policy, and two revised privacy policy instructions this year.

- **New:** *Privacy Incident Responsibilities and Breach Response Team* establishes DHS policy, responsibilities, and requirements for responding to all incidents involving PII contained in DHS information; and establishes the requirement for the Chief Privacy Officer (CPO) to convene and lead a Breach Response Team when a “major incident” involving PII has occurred,⁹ or at the discretion of the CPO.
- **Revised:** *Privacy Incident Handling Guidance* (PIHG) establishes DHS policy for responding to privacy incidents by providing procedures to follow upon the detection or discovery of a suspected or confirmed incident involving PII in an unclassified environment.
- **Revised:** *Handbook for Safeguarding Sensitive PII* provides best practices and DHS policy requirements to prevent a privacy incident involving Sensitive PII during all stages of the information lifecycle: *when collecting, storing, using, disseminating, or disposing of Sensitive PII.*



⁹ A breach constitutes a “major incident” when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals’ PII constitutes a “major incident,” as defined in OMB M-18-02. The CPO, in coordination with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO), will first determine whether a privacy incident is considered a “major incident” that involves PII.

Privacy Policy Leadership

During the reporting period, the Privacy Office provided significant privacy policy leadership on a wide range of topics in various fora, as described below in alphabetical order. For each, the related core DHS mission is indicated.

Cybersecurity

The Privacy Office meets regularly with the National Protection and Programs Directorate's (NPPD) Office of Privacy, Office of Cybersecurity & Communications (CS&C), and its National Cybersecurity and Communications Integration Center (NCCIC) to discuss ways to effectively integrate privacy protections into the Department's cybersecurity activities, and embed privacy safeguards into the technologies being deployed for cyber detection and prevention. The Privacy Office also supports the drafting of privacy compliance documentation related to DHS cyber programs, and oversees the Data Privacy and Integrity Advisory Committee's cyber subcommittee.



The Privacy Office continues to work closely with NPPD on the Department's various cybersecurity initiatives, including the implementation of the Cybersecurity Information Sharing Act (CISA), the Automated Indicator Sharing (AIS) Initiative, the EINSTEIN programs,¹⁰ all cyber-related Executive Order activities/deliverables under Executive Orders 13636, 13691, and 13800, as well as legislative and programmatic reviews, as appropriate. Further, the Privacy Office and Office for Civil Rights and Civil Liberties (CRCL) coordinate with the Interagency to draft and publish the annual Executive Order 13636/13691 Privacy and Civil Liberties Assessments Report. *Mission Number Four: Safeguard and Secure Cyberspace.*

Cybersecurity Information Sharing Act (CISA) of 2015 Periodic Joint Review of Privacy and Civil Liberties Guidelines

The CPO worked closely with the NPPD Office of Privacy, CRCL, and the Justice Department on the 2018 Periodic Joint Review of the Privacy and Civil Liberties Guidelines contained in the CISA. These Guidelines establish the privacy and civil liberties requirements governing the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with the activities authorized by CISA, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats, any other applicable provisions of law, and the FIPPs. The 2018 Period Joint Review consisted of only minor administrative changes, to include updating outdated language within the guidelines, and clarifying federal entities' ability to develop supplemental guidelines relative to cyber threat

¹⁰ Find the EINSTEIN PIAs here under Cybersecurity-related PIAs: <https://www.dhs.gov/privacy-documents-national-protection-and-programs-directorate-nppd>

indicators and defensive measures as long as they do not circumvent or otherwise supersede the Privacy and Civil Liberties Final Guidelines.

Executive Order 13800 “Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”

On May 11, 2017, President Trump issued Executive Order 13800 (EO 13800), *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, to improve the Nation’s cyber posture and capabilities in the face of intensifying cybersecurity threats to its digital and physical security. EO 13800 initiates action on four fronts:

1. It secures the federal networks that operate on behalf of the American people.
2. It encourages collaboration with industry to protect critical infrastructure that maintains the American way of life.
3. It strengthens the deterrence posture of the United States and builds international coalitions.
4. It places much needed focus on building a stronger cybersecurity workforce, which is critical for the Nation’s long-term ability to strengthen its cyber protections and capabilities.

In order to carry out these actions, the Department has established several internal DHS Working Groups. The Privacy Office participates as a working member in each of these groups and ensures that privacy protections are preserved, and any privacy concerns are identified and mitigated before any action or initiative is implemented.

Data Framework

DHS developed the Data Framework as a scalable information technology (IT) program with built-in capabilities to support advanced data architecture and governance processes. The Data Framework is DHS’s big data solution, and includes robust privacy protections and oversight while facilitating more controlled, effective, and efficient use and sharing of existing homeland security-related information across the DHS enterprise, as well as with other U.S. Government partners, as appropriate.

The Data Framework, comprised of the Neptune and Cerberus Systems,¹¹ uses data tags to apply policy-based rules to determine which users can access which data for what purpose, so that DHS can share its information internally while protecting privacy through robust policy and technical controls. In the first quarter of 2018, the Data Framework continued its progression towards Full Operational Capability (FOC) by completing its critical refresh. This refresh enhanced system performance for future scalability, adding additional data sets, improving data quality and usability, supporting DHS sharing with the Intelligence Community, and developing a governance process to approve the use of analytical tools on Framework data.

¹¹ See [DHS/ALL/PIA-046](#)

The Privacy Office facilitates the preservation of privacy protections in the Data Framework through the:

- requirement of Privacy Threshold Analysis (PTA) submissions for each dataset targeted for onboarding, as well as updates to the Data Framework PIA and SORN for each dataset on boarded for any new use or user of a dataset. The Privacy Office uses the PTA, in part, to determine if access control rules and user access controls are sufficient;
- Data Framework Working Group (DFWG), of which the Privacy Office is a member, approves all datasets ingested, and the requestors must provide an articulated use that is consistent with the use or uses approved by the IT source system; and
- Data Access Request Council (DARC), of which the Privacy Office is a member, must approve all external bulk transfers of data to ensure any information sharing is governed by the appropriate Information Sharing and Access Agreement (ISAA) that accounts for records access and the purpose for access.

The Privacy Office performs a significant oversight role as datasets are prioritized, tagged, and moved into the Data Framework, and as new analysis tools are deployed. *Mission Number One: Prevent Terrorism and Enhance Security.*

Deputy Secretary's Management Action Group

The Deputy CPO participates in the Deputy Secretary's Management Action Group (DMAG), a senior leadership body that allows for candid discussion and transparent, collaborative, and coordinated decision making on a wide range of matters pertaining to DHS enterprise management, including emerging issues, joint operational requirements, program and budget review, acquisition, and operational planning.

The Privacy Office supports the Joint Requirements Council (JRC), which reports to the DMAG and serves as an executive level body that provides oversight of the DHS operational requirements generation process, harmonizes efforts across the Department, and makes prioritized funding recommendations to the DMAG for those validated operational requirements. The JRC is also responsible for examining what tools and resources the Department needs in order to operate in the future across a wide variety of mission areas, including aviation fleet; screening and vetting; information sharing systems; chemical, biological, radiological, and nuclear detection; and cybersecurity. *Mission cross-cutting goal: To mature and strengthen homeland security by integrating information sharing and preserving privacy, oversight, and transparency in the execution of all departmental activities.*

Federal Acquisition Regulation (FAR) Clauses

The Privacy Office is currently involved in three separate interagency Federal Acquisition Regulation (FAR) efforts that have not been finalized:

1. The first effort involves the ongoing work to implement a FAR clause to address the reporting requirements of OMB Memorandum M-17-12, “*Preparing for and Responding to a Breach of Personally Identifiable Information*.” This clause requires contractors and subcontractors who collect, maintain, use, share or dispose of PII on behalf of the government, or who operate an information system on behalf of the government that may have PII residing in or transiting through the information system, to provide adequate security and privacy protections for such information, and rapidly report any breach in accordance with the clause. Development of the FAR clause was the first step in the implementation process. Oversight efforts continue until the clause is included in all contracts and agreements.
2. Second, the Privacy Office continues to take part in an interagency working group to amend the FAR to implement the Federal Controlled Unclassified Information (CUI) Program. The CUI program affects all organizations that handle, possess, use, share or receive CUI, including federal contractors. The Privacy Office continues to support this effort while ensuring that sensitive information, including PII, is appropriately safeguarded throughout the data lifecycle.
3. Finally, the Privacy Office is part of an interagency effort to develop a process to determine when a stop work order for DHS contracts should be issued (and later lifted) after receiving an incident notification. This process will also identify whether all or part of the contractor’s scope of work is affected during the stop work period. The Privacy Office’s focus is the preservation of forensic information and the ability to work with the contractor to investigate, mitigate, and remediate a privacy incident, pursuant to OMB guidance and DHS policy.¹²

Freedom of Information Act (FOIA)

The Privacy Office has made significant strides in implementing each of the procedural amendments in the *FOIA Improvement Act of 2016*¹³ (the Act):

- On February 20, 2018, the Privacy Office issued [Instruction 262-11-001, Freedom of Information Act Compliance on Employee Notification](#) to formalize an employee notification process to inform current Department employees when their employment records, as defined in the instruction, are about to be released under the FOIA.
- In last year’s report, the Privacy Office reported that on April 17, 2017, the Acting Under Secretary for Management signed the new [Directive 262-11, Freedom of Information Act Compliance](#) to clarify the roles and responsibilities of the Chief FOIA Officer, the Deputy Chief FOIA Officer, Component FOIA Officers, and other officials with FOIA responsibilities. During this reporting period, the Privacy Office revised portions of the Directive, and circulated the draft for Component review.

¹² See: OMB M-17-12 and OMB M-18-02, and DHS Privacy Policy Instruction 047-01-006 Privacy Incident Responsibilities and Breach Response Team, DHS Privacy Policy Instruction 047-01-007 Handbook for Safeguarding Sensitive PII, and DHS Privacy Policy Instruction 047-01-008 Privacy Incident Handling Guidance.

¹³ *FOIA Improvement Act of 2016* (Public Law No. 114-185).

-
- The Privacy Office will create additional instructions to supplement the directive to improve the Department's compliance with FOIA and adherence to DHS FOIA policy. Two new instructions are in review now. One addresses FOIA reporting requirements, and another a requirement to have each Component appoint a Component FOIA Officer within their organization to oversee FOIA administration, compliance, policy, and oversight activities in coordination with the Chief FOIA Officer.

Mission cross-cutting goal for FOIA: To mature and strengthen homeland security by preserving transparency in the execution of all departmental activities.

Fusion Centers

In 2007, the *Implementing Recommendations of the 9/11 Commission Act* (9/11 Commission Act) established the DHS State, Local, and Regional Fusion Center Initiative, thereby codifying an existing relationship between DHS and a national network of fusion centers. The Privacy Office has exercised leadership in establishing and growing a robust privacy protection framework within the fusion center program, both at the national and state levels. The Privacy Office reviews all fusion center privacy policies to ensure that they are as comprehensive as the [Information Sharing Environment \(ISE\) Privacy Guidelines](#). The Privacy Office also collaborates with CRCL and the Office of Intelligence and Analysis (I&A) State and Local Partner Engagement Office to train fusion center privacy officers and analytical staff.

Mission Number One: Prevent Terrorism and Enhance Security.

Insider Threat Program

The Privacy Office participates in the operation of the Department's Insider Threat Program (ITP) in several ways. Department-wide and Component-specific ITP activities are subject to the Department's privacy compliance documentation requirements. Privacy Office staff also participate in the Insider Threat Working Group (ITWG), which provides coordination, planning, and policy development for the Department and all its Components. In addition,



Privacy Office staff play a central role on the Insider Threat Oversight Group (ITOG).

The ITOG's primary purpose is to review all policies and programs used at DHS that monitor for threats to DHS personnel, facilities, resources, and information systems. The group includes the Office of General Counsel's Intelligence Law Division, the Office for Civil Rights and Civil Liberties, and the Privacy Office. The ITOG meets quarterly to review the quarterly reports that provide anonymized details of all ITP activities and investigations, and makes recommendations for new policies or procedures based on its review of the quarterly reports. The ITOG also meets as needed to discuss new user activity monitoring policies and to authorize enhanced user activity monitoring of individuals who appear to pose an insider threat to DHS. Privacy Office staff are also working with the other members of the ITOG to finalize auditing procedures. The ITWG was created to help implement insider threat user activity monitoring at all DHS

Components and offices. It is comprised of the Component Insider Threat Officials, the Senior Insider Threat Official (SITO) and his staff, the ITOG, and subject matter experts from other offices as deemed necessary by the SITO. Privacy Office staff attend all meetings and advise members on drafting compliance documents, establishing appropriate oversight processes, and resolving privacy concerns as they arise. *Mission Number One: Prevent Terrorism and Enhance Security.*

Screening and Vetting Initiatives

To identify and mitigate privacy concerns that may arise from the implementation of Executive Order 13780, “*Protecting the Nation from Foreign Terrorist Entry into the United States,*” and other recent proposals for enhanced screening and vetting measures, the Privacy Office began participating in several intra- and inter-agency working groups and meetings. Two such initiatives are related to the implementation activities associated with National Security Presidential Memorandum (NSPM) -7 and NSPM-9.

NSPM-7, *Integration, Sharing, and use of National Security Threat Actor Information to Protect America*, issued October 4, 2017, established five categories of national security threat actors (NSTA), and directs the development of technical architectures and policy frameworks to advance data integration and sharing of identity attributes (i.e., Cyber, Foreign Intelligence, Military, Transnational Organized Crime, and Weapons Proliferators).

Each NSTA phase will require privacy oversight. The Department’s mission is to support the national vetting enterprise, to vet across multiple holdings, eliminate stove-piped architectures, and to standardize records for easy correlation. The Privacy Office will help bring the Department into compliance with EO 13780 and NSPM-7 by analyzing sharing requirements, advising on data stewardship, overseeing the training of DHS employees on best practices as they relate to the FIPPs, and collaborating and building privacy into the technical architecture needed to increase sharing and integration with other U.S. Government stakeholders. The Privacy Office continues to attend working group meetings to monitor the progress of the NSPM-7 Implementation Plan.

NSTA derogatory data will also be shared with the Intelligence Community (IC), consistent with applicable authorities. In addition, the IC will be a source for DHS NSTA. As the Department leverages its border and port data collection expertise and its broad authorities, the Privacy Office will lend its experience in FOIA, records management, and redress. At the core of NSPM-7 is the collection, use, and sharing of accurate, complete, and timely NSTA data. The Privacy Office will make every effort to ensure that all DHS proposals include the implementation of solid data protection strategies.

NSPM-9, *Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise*, issued February 6, 2018, directed the Secretary of Homeland Security, in coordination with the Secretary of State, the Attorney General, and the Director of National Intelligence, to establish the National Vetting Center (NVC) which is designed to improve the efficiency and effectiveness of U.S. Government vetting programs to better identify individuals who may pose a threat to national security, border security, homeland security, or public safety, consistent with law and policy. NSPM-9 establishes a policy to use intelligence and law

enforcement information, as authorized by existing law, in support of adjudications or other decisions that occur in the immigration and border security areas.

The Privacy Office is directly engaged in oversight and governance efforts related to NSPM-9 and creation of the NVC. NSPM-9 required the establishment of the National Vetting Governance Board to serve as the senior interagency forum for considering issues that affect the national vetting enterprise and the activities of the Center, and a standing Privacy, Civil Rights and Civil Liberties (P-CRCL) Working Group to ensure that the activities of the Board and the Center appropriately protect individuals' privacy, civil rights, and civil liberties. The CPO serves as a co-chair of the P-CRCL Working Group, which is comprised of senior privacy and civil liberties officials from several departments and agencies supporting the implementation of NSPM-9. Privacy Office staff also serve on the Working Group, which meets regularly to evaluate various aspects of the NVC's plans for implementation, and provide advice and guidance to the NVC and the Board. The CPO also represents the P-CRCL Working Group as an *ex officio*, non-voting member of the Governance Board.

The Privacy Office, through its role on the P-CRCL Working Group, has been engaged in reviews and activities designed to incorporate privacy into NVC technology and business processes. In addition to reviewing drafts of the Implementation Plan for the NVC, the Working Group is also involved in evaluating and providing input into the Concept of Operations document which details NVC's operational and technical model. The Working Group conducted a FIPPs-based risk assessment of the draft Implementation Plan for the NVC and presented it to the Governance Board in June 2018. The Working Group has also drafted technical requirements focusing on data quality, access control, data retention, and transparency, for the various technologies that will be used when NVC becomes operational.

To support efforts to create the NVC, the CPO and the DHS Officer for CRCL recruited a senior executive from a DHS Component privacy office to serve as the P-CRCL Advisor to the NVC during its implementation period. This temporary position serves as a full-time advisor to the NVC leadership and incorporates privacy, civil rights, and civil liberties protections into all aspects of planning for the NVC. The NVC is expected to hire a permanent P-CRCL officer later in 2018.

DHS will build new technology that NVC will offer to facilitate improved vetting for various immigration and border security programs. The Privacy Office will provide oversight and ensure compliance with the FIPPs and key privacy laws and policies as the NVC is being created within DHS, and as new DHS technology is deployed to support the NVC mission. The Privacy Office is also providing appropriate levels of public transparency by preparing a Privacy Impact Assessment (PIA) for the NVC, which will be released to the public before the NVC begins operations.

In addition to its roles and activities associated with the implementation of NSPMs 7 and 9, the Privacy Office is also a voting member of the DHS Shared Services Vetting Board, which seeks to define and develop how DHS vets travelers across the enterprise. *Mission Number One: Prevent Terrorism and Enhance Security.*

Social Media Task Force

The Privacy Office is a member of the DHS Social Media Task Force (Task Force), designated to oversee, coordinate, and facilitate Department use of social media information in furtherance of DHS and operational Component missions.



DHS uses social media to meet its missions:

1. Public Affairs: push out information; no PII collected;
2. Situational awareness: passive observation; no PII collected;
3. Operational use: varies based on authorities; majority of DHS social media collections are for operational use; and
4. Intelligence: pursuant to Executive Order 12333.

Using social media appropriately in the context of the Department's operational missions has many potential benefits, but also presents risks to privacy. Because of this, the Privacy Office continues to work closely with the members of the Task Force to assess capabilities and critical mission needs in order to identify and mitigate privacy concerns regarding current and future desired capabilities. The Privacy Office further requires DHS Components to complete a Social Media Operational Use Template (SMOUT) request¹⁴ that is based on mission-specific authorities reviewed and approved by Component Counsel, documented by the Component Privacy Officer or PPOC, and approved by the CPO. Further, all PII collected through the Operational Use of Social Media must be consistent with the approved category of use and with the applicable System of Records Notice(s) (SORN). *Missions One and Two: Prevent Terrorism, Enhance Security, and Secure and Manage Our Borders.*

Terrorist Prevention Working Group (TPWG)

The Privacy Office is involved in the Department's terrorism prevention activities primarily through participation in the Office of Terrorism Prevention's Terrorism Prevention Working Group (formerly Countering Violent Extremism Working Group). We review proposed research and programs, along with work product, prior to completion to ensure that the Department's terrorism prevention work is consistent with applicable privacy law and policy. *Mission Number One: Prevent Terrorism and Enhance Security.*

¹⁴ In accordance with Directive 110-01, Privacy Policy for Operational Use of Social Media (June 8, 2012) and Instruction 110-01-001.

Unmanned Aircraft Systems (UAS)

The Privacy Office plays a role in developing UAS compliance documentation, promoting transparency so the public understands DHS's use of UAS, ensuring DHS UAS policy is privacy-sensitive, reviewing grant proposals from state, local, tribal, and territorial (SLTT) agencies that wish to acquire small UAS (sUAS), and developing policies and procedures to help counter threats to the Homeland from the use of UAS by our adversaries.



Whenever the DHS Components consider the acquisition, development, or deployment of UAS, they must first complete a PTA. The purpose of most of the UAS PTAs reviewed by the Privacy Office are testing or demonstration. In these cases, Privacy Office staff work with the Component(s) to determine if any individuals outside of DHS may find their privacy encroached upon during the test or demonstration flights. In most cases, such flights are held in areas restricted to the public and are conducted without the use of sensors that might obtain PII. In those cases in which there is even a remote possibility that UAS operation, or the use of counter-UAS technology, may result in DHS acquiring PII, the Privacy Office requires a PIA. To date, the Privacy Office has published three PIAs for three different components: the [Science and Technology Directorate in 2012](#), [U.S. Customs and Border Protection in 2013](#), and the [U.S. Secret Service in 2017](#).

The Privacy Office works with CRCL to evaluate SLTT requests to use preparedness grant funding administered by the FEMA Grant Programs Directorate to acquire sUAS, as required by the Presidential Memorandum on “*Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*” (Section 1(c)(vi)). The Privacy Office has, in concert with CRCL, reviewed twenty-three such requests during the current reporting period. One is currently on hold pending submission of additional material at the request of the Privacy Office; seven were cleared after submitting additional material. The Privacy Office cleared the remaining requests without requiring additional information. In all cases, we provide SLTTs with links to the [Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft Systems Programs](#) and the “Presidential Memorandum” for their use in further developing their programs.

The Privacy Office is involved in several intra- and inter-agency working groups that are attempting to determine the appropriate methods and policies to interdict, redirect, or otherwise interrupt the flight of UAS encroaching on restricted airspace, hazarding protective operations, or potentially causing harm to critical infrastructure or key resources. There is a perceived risk that counter-UAS operations might interfere with the innocent flight of UAS, and during such counter-UAS operations, DHS might gain access to PII. The Privacy Office is diligently working with its partners to develop suitable policies and procedures to minimize the possibility that a DHS Component would inappropriately gain access to a person's PII. This is an ongoing project that requires additional policy development, technology testing and evaluation, and possibly, legislation. *Mission Number Two: Secure and Manage Our Borders.*

Violence Against Women Act: A Holistic Approach to Protecting the Information of Victim Immigrants

In the the 2018 *Consolidated Appropriations Act*,¹⁵ Congress provided the Privacy Office with additional funding to ensure information and data released by the Department does not reveal the identity or PII of non-U.S. Persons who may be survivors of domestic violence, sexual assault, stalking, human trafficking, or other crimes. The confidentiality protections afforded to alien victims of crimes are statutorily required under Title 8, United States Code, Section 1367, *Violence Against Women Act* (herein Section 1367). The DHS Officer for CRCL has, through Secretarial delegation, the authority to provide DHS-wide guidance and oversight on the implementation of Section 1367 confidentiality and prohibited source provisions. The Chief Privacy Officer must determine any potential impacts a privacy incident may have on the privacy of individuals, including those protected by Section 1367. Because of the shared responsibilities for ensuring the proper handling of Section 1367 information, in FY 2018 the Privacy Office and CRCL developed a process for the two offices to share incidents of unauthorized Section 1367 disclosures and partner to ensure incidents are appropriately reviewed, investigated, addressed, and resolved.

During the reporting period, the Privacy Office hosted two Special Protected Classes Unauthorized Disclosure forums to refresh and educate the PPOCs and Incident Practitioners. Section 1367 incident reporting has increased, which is a positive indicator that the department-wide outreach is taking effect. The team oversight approach produces effective solutions, and is proving to be a constructive mechanism overall.

In May 2018, the Chief Privacy Officer initiated a Privacy Compliance Review (PCR) of Privacy Incidents Affecting Individuals Protected by Section 1367, focused on those Components and offices most likely to access or be responsible for dissemination of Section 1367 records: United States Immigration and Customs Enforcement (ICE), CBP, U. S. Citizenship and Immigration Services (USCIS), NPPD's Office of Biometric Identity Management (OBIM), and I&A. The forthcoming PCR will identify and mitigate risks that may be incurred with the inadvertent disclosure of alien victims' protected information.

The Chief Privacy Officer also reviewed relevant Privacy Impact Assessments (PIA) and ISAAs to ensure the inclusion of language to protect Section 1367 records. And the Privacy Office is developing instructions to disseminate to FOIA professionals that will outline the withholding requirements of this information.

Mission cross-cutting goal: To mature and strengthen homeland security by integrating information sharing and preserving privacy, oversight, and transparency in the execution of all departmental activities.

¹⁵ Pub.L. 115-141



II. Outreach, Education, and Reporting

The Privacy Office's FY 2015-2018 Strategic Plan includes four strategic goals:

Goal Two (Education and Outreach): Provide outreach, education, training, and reports in order to promote privacy and transparency in homeland security.

The Privacy Office continues to look for ways to promote transparency and engage with the privacy advocacy community, international partners and stakeholders, and the public. Engagement methods include public workshops, the Privacy Office website, the Federal Privacy Council's Federal Privacy Summit, and Privacy Office leadership and staff appearances at conferences and other fora. In addition, the CPO and Deputy CPO host periodic informational meetings with members of the privacy advocacy community to inform them of key privacy initiatives throughout the year. Further, the Privacy Office participates in public and private meetings with the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the Executive Branch, and the DHS Data Privacy and Integrity Advisory Committee (DPIAC).

Outreach

Conferences and Events

Privacy Office staff present at conferences and participate in public meetings to educate and inform both the public and private sectors on DHS privacy and disclosure policies and best practices.

- ***American Society of Access Professionals Tenth National Training Conference*** – In July 2017, the Privacy Office hosted a DHS-specific block of instruction regarding the DHS perspective on a variety of topics, including FOIA Exemptions 4 and 7, and DHS’s role in the FOIA Advisory Committee.
- ***Federal Privacy Council’s Monthly Training Series*** – On September 28, 2017, in Washington, DC, the Federal Privacy Council hosted a seminar entitled *Privacy versus Security*. Panelists included the Deputy CPO and the Deputy Chief Information Security Officer.
- ***Federal Privacy Summit*** – On December 12, 2017, in Washington, DC, the Federal Privacy Council hosted a one-day workshop that convened privacy professionals from over 20 federal agencies to discuss privacy and security best practices. Subject matter experts, including the CPO and the Deputy CPO, shared best practices for protecting privacy, and ways to improve collaboration across the enterprise.
- ***The Office of the Director of National Intelligence (ODNI)*** – On January 24, 2018, in McLean, VA, ODNI hosted a privacy seminar at which the CPO participated in a panel discussion, *Balancing Privacy and National Security: Privacy Officer Perspectives*.
- ***DHS Sunshine Awards*** – On March 16, 2018, the former DHS Deputy Secretary, Elaine Duke, and the Chief FOIA Officer recognized four FOIA professionals for their work and dedication to FOIA operations. The event included opening remarks from the Chief FOIA Officer and a keynote address from the Deputy Secretary on the importance of the FOIA in providing transparency and openness into the Department’s law enforcement mission.
- ***The International Association of Privacy Professionals (IAPP) Global Summit*** – On March 27 - 28, 2018, in Washington, DC, the CPO interviewed CBP’s Deputy Assistant Commissioner on border security and privacy, and the Deputy CPO participated on a panel, *How to Get a Privacy Job in the Federal Government*.
- ***Legal and Policy Seminar sponsored by Thompson Hine, LLP*** – On May 8, 2018, in Washington, DC, the CPO gave the keynote address on *How to Establish an Effective Privacy Program*.
- ***Department of Justice Privacy Training*** – On May 15, 2018, in Washington, DC, the CPO participated in a panel discussion on international privacy issues, including the U.S. – European Union (EU) Passenger Name Record (PNR) Agreement, the National Vetting Center, and the European Union’s General Data Protection Regulation (GDPR) impact on DHS.
- ***American Society of Access Professionals Eleventh National Training Conference*** – In July 2018, in Arlington, VA, the CPO gave a speech on how DHS is improving FOIA responsiveness and performance to meet increasing demand.

-
- **Chief FOIA Officers Council Meeting** – On July 19, 2018, in Washington, DC, the CPO spoke on how DHS has overcome challenges in FOIA administration and capitalized on new opportunities.

In addition, the Privacy Office and the Component FOIA Offices serve on various panels outside the Department that enable them to: (1) standardize FOIA best practices across the Department; and (2) promote transparency and openness within DHS and among the requester community.

The Chief FOIA Officer and the Deputy Chief FOIA Officer are members of the Chief FOIA Officer Council¹⁶ and participate in meetings with the requester community to develop recommendations for increasing FOIA compliance and efficiency, disseminating information about agency experiences and best practices, and working on initiatives that will increase transparency.

Federal Privacy Council

The Federal Privacy Council (Privacy Council) was established by presidential [Executive Order 13719](#) in 2016 to serve as an interagency forum for Senior Agency Officials for Privacy (SAOP) to share best practices and develop procedures to protect privacy, to expand the skill and career development opportunities of agency privacy professionals, and to promote collaboration between and among agency privacy professionals to reduce unnecessary duplication of efforts.



In 2016, the Council created the first website, www.fpc.gov, to feature privacy laws, regulations, and resources for public sector privacy professionals.

Senior Privacy Office staff worked with OMB to stand up the Federal Privacy Council and draft its charter and by-laws. Privacy Office and Component privacy office staff support the following Federal Privacy Council committees and subcommittees, and help plan its annual Federal Privacy Summit. The Privacy Office has in recent months helped spearhead an interagency effort to assess the impact on federal agencies of the European Union’s new General Data Protection Regulation (GDPR).

The Privacy Council’s working committees include:

- **Federal Privacy Workforce Committee:** This Committee addresses the myriad challenges SAOPs face in fostering an effective and efficient workforce that enables agency mission success. These challenges include: identifying people with the critical skills, knowledge, and

¹⁶ The FOIA Improvement Act of 2016 (Public Law No. 114-185) created a new Chief FOIA Officer Council within the Executive Branch that will serve as a forum for collaboration across agencies and with the requester community to explore innovative ways to improve FOIA administration.

experience needed in today's tech-driven and big data environment; hiring the right people at the right time; retaining high-performing people; training and maintaining a skilled, diverse workforce; promoting professional development and career advancement opportunities for privacy professionals; and ensuring the government is staffed with the best privacy professionals to enable agencies to manage unprecedented volumes of PII and properly protect individuals' privacy.

- **Technology and Innovation Committee:** To continue the transformation to a 21st century government that serves the American people more effectively, agencies must embrace and leverage cutting-edge technologies, new digital services, and advances in data analytics. This Standing Committee addresses issues at the intersection of privacy, technology, and policy with the overall goal of promoting innovation and enabling the wide-scale adoption of new technologies and services. Issues that the Committee may consider addressing include: big data analytics, cloud computing, de-identification of data, mobile applications, social media and digital services, Internet of Things, artificial intelligence, unmanned aerial systems, and new technologies and tools for securing information assets. In each case, the Committee will examine privacy risks related to new technologies and practical approaches for mitigating those risks consistent with laws, guidance, policy, and best practices.
- **Agency Implementation Committee:** This Standing Committee's mission is to address the numerous challenges related to privacy program governance and privacy risk management for federal agencies. Members of this Standing Committee address issues including the development of data governance and compliance strategies for PII, evaluation of different models for privacy program organization and implementation, assessing privacy program success and maturity, privacy risk management, information sharing and dissemination, and breach response. Challenges related to legal compliance with privacy laws, guidance, and other requirements, as well as other overarching challenges and privacy program requirements that are common to most agencies, fall within the scope and mission of this Committee. This Committee sponsors an eight-week Privacy Boot Camp training course for new privacy professionals in the Federal Government.

Data Privacy and Integrity Advisory Committee

The DHS Data Privacy and Integrity Advisory Committee (DPIAC) provides advice to the Department at the request of the CPO on programmatic, policy, operational, administrative, and technological issues within DHS that relate to PII, data integrity, and other privacy-related matters.¹⁷ DPIAC members have broad expertise in privacy, security, and emerging technology, and come from large and small companies, the academic community, and the non-profit sector. Members hold public meetings to receive updates from the Privacy Office on important privacy issues, and to deliberate taskings from the CPO.

¹⁷ The Committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. § 451 and operates in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App 2. DPIAC members serve as Special Government Employees and represent a balance of interests on privacy matters from academia, the private sector (including for-profit and not-for-profit organizations), state government, and the privacy advocacy community.

-
- On September 19, 2017, in Washington, DC, the Privacy Office hosted a public meeting of the DPIAC. Members were briefed on biometrics, facial recognition, and immigration data, and tasked with submitting a report on best practices for protecting immigration statistics.
 - On May 22, 2018, the NPPD Office of Privacy hosted a meeting with the DPIAC's Cyber Subcommittee and the leadership of the NPPD Office of Cybersecurity and Communications (CS&C) to provide an update on recent privacy projects and initiatives at CS&C. The meeting also included an open discussion on the potential effects of the European Union's General Data Protection Regulation (GDPR) on the NPPD cyber mission.
 - On July 10, 2018, members of the DPIAC's Policy Subcommittee, along with officials from the DHS Privacy Office and CBP's Offices of Privacy and Field Operations, toured biometric entry and exit operations at Orlando International Airport to observe general passenger processing operations, including pilot entry and exit programs. Attendees were briefed on data collection, uses, and sharing associated with the entry processing of arriving visitors, as well as a pilot program in which CBP has collaborated with British Airways to use biometric data (facial images) to verify a traveler's identity and process them for exit. The pilot utilizes an e-gate in the boarding area of the departure terminal, and allows passengers to board their flight without presenting any travel documentation or a boarding pass. Back-end programming uses images captured at the gate to instantaneously match the individual to a gallery or previously captured images in order to verify their identity, and match it to flight information. The CBP Privacy Office was able to verify that proper notification of the information collections, including signage, was in place, and that travelers were made aware that participation in pilot activities was optional.

All DPIAC reports, along with membership and meeting information, are posted on the Privacy Office website: www.dhs.gov/privacy.

Privacy Advocates

The CPO and Deputy CPO host periodic informational meetings with members of the privacy advocacy community to inform them of key privacy initiatives throughout the year.

Biometrics/Facial Recognition: On August 1, 2017, at CBP Headquarters in Washington, D.C., the CPO, Deputy CPO, and CBP's Deputy Executive Assistant Commissioner of Field Operations conducted an information sharing session and open dialogue about CBP's implementation plans for a biometric exit system with external privacy stakeholders. With the recent support from Congress in the Consolidated Appropriations Act, 2016 (Pub. L. No. 114-113), and at the direction of the President in section 8 of Executive Order 13780, *Protecting the Nation from Foreign Terrorist Entry into the United States*, CBP is making significant progress toward implementation of a biometric exit system.

Cybersecurity: On May 11, 2018, the NPPD Office of Privacy and CRCL held a briefing for the privacy and civil liberties advocacy community to provide updates on the National Cybersecurity and Communications Integration Center's (NCCIC) cyber programs, the Automated Indicator Sharing (AIS) Initiative, NPPD's continued work to improve election security, and the biennial review of the CISA Privacy and Civil Liberties Final Guidelines.

NSPM-9/National Vetting Center: On April 5, 2018, the National Vetting Governance Board’s Privacy, Civil Liberties, and Civil Rights Working Group, of which the Chief Privacy Officer is a co-chair, held a listening session attended by civil liberties, civil rights, and privacy advocacy organizations. The purpose was to hear questions and concerns about NSPM-9 and the National Vetting Center, while plans for implementation were still being developed. The meeting was attended by the Senior Agency Officials for Privacy from the Departments of State, Defense, and Justice, the Central Intelligence Agency, the Federal Bureau of Investigation, and the Office of the Director for National Intelligence. The government representatives gave an overview of NSPM-9, and addressed questions about its scope and possible application to various immigration and border security programs.

Privacy and Civil Liberties Oversight Board

The Privacy Office participates in public and private meetings with the Privacy and Civil Liberties Oversight Board (PCLOB), which was established as an independent oversight board within the Executive Branch by the Implementing Recommendation of the 9/11 Commission Act. Examples of Privacy Office collaboration with the PCLOB during this reporting period include:

- *Data Framework Oversight Project:* The Privacy Office, in coordination with CRCL and the Office of the General Counsel (OGC), continues to support an ongoing oversight project conducted by the PCLOB. As a part of this project, the PCLOB is reviewing the design and counterterrorism-related uses of the DHS Data Framework. DHS oversight includes the system rules for permitting access to information, the system’s analytical capabilities, including data mining, and any related dissemination of information. PCLOB’s review focuses on the use of datasets that are already incorporated into the system and the compliance and oversight capabilities that have been implemented.
- *Privacy and Civil Liberties Assessment Report:* The Privacy Office worked closely with the PCLOB to draft this annual report, which is required by Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*.

International Engagement & Outreach

DHS works closely with international partners, including foreign governments and major multilateral organizations, to strengthen the security of the networks of global trade and travel upon which the Nation’s economy and communities rely. When those engagements involve sharing PII, the Privacy Office reviews information sharing arrangements to ensure that the DHS position is consistent with U.S. law and DHS privacy policy.

During the reporting period, the Privacy Office met with 11 representatives from Germany, Israel, and France. These engagements increased understanding of the U.S. privacy and FOIA frameworks, DHS privacy and disclosure policy, privacy compliance, information sharing, and cybersecurity. By sharing DHS privacy compliance and policy practices with international partners and promoting the FIPPs, the Privacy Office conveys privacy best practices, and builds the confidence necessary for cross-border information sharing and cooperation.

In addition, the Privacy Office participates in the Department's International Pre-Deployment Training, a week-long training course for new DHS attachés deployed to U.S. embassies worldwide. The Privacy Office provides an international privacy policy module to raise awareness of the potential impact of misperceptions regarding DHS privacy policy, practice, and global privacy policies on DHS's international work.

Education: Privacy & FOIA Training and Awareness



The Privacy Office develops and delivers a variety of ongoing and one-time privacy and transparency-related training to DHS personnel and key stakeholders. Since most privacy incidents are accidental, staff training and awareness are key to prevention. We want all personnel to understand, identify, and mitigate privacy risks, and proactively safeguard PII.

- Privacy Office and Component privacy training and awareness activities are detailed in the *Privacy Office Semi-Annual Reports to Congress*, available on our website.
- Privacy Office and Component FOIA training and awareness activities are detailed in the annual *Chief Freedom of Information Act (FOIA) Officer Report to the Attorney General of the United States*, also available on our website.

Key training programs are highlighted below.

Mandatory Online Privacy Training

Each year, DHS personnel complete a mandatory online privacy awareness training course, [Privacy at DHS: Protecting Personal Information](#). This course is required for all personnel when they join the Department, and annually thereafter.

Classroom Privacy and FOIA Training

New Employee Orientation: The Privacy Office provides privacy and FOIA training as part of the Department’s bi-weekly orientation session for all new DHS Headquarters employees. Many of the Component Privacy Officers also offer privacy training for new employees when they onboard. In addition, the Privacy Office provides privacy training as part of the quarterly two-day course, *DHS 101*, an overview of all DHS Components.

FOIA Training

The FOIA Improvement Act of 2016 requires that the agency Chief FOIA Officer “offer training to agency staff regarding their FOIA responsibilities.”¹⁸ The Privacy Office and the Component FOIA Offices conduct internal staff training to standardize FOIA best practices across the Department, and to promote transparency and openness within DHS and among the requester community.

All DHS Headquarters personnel and most Component staff receive FOIA training as part of New Employee Orientation. This initial FOIA training is reinforced through mandatory online annual instruction in records management that also addresses staff FOIA responsibilities.

¹⁸ 5 U.S.C. § 552 (j)(2)(F).

The Privacy Office also conducts periodic classroom FOIA training for agency staff regarding their responsibilities under the FOIA. During the reporting period, the Privacy Office:

- Hosted a DHS-specific block of instruction regarding the DHS perspective on a number of topics at the American Society of Access Professionals (ASAP) National Training Conference. The block included presentations from the FEMA Chief FOIA Officer regarding Exemption 4, the USCIS Chief FOIA Officer regarding DHS's role in the FOIA Advisory Committee, and the ICE Chief FOIA Officer regarding Exemption 7.
- Partnered with the Office of Government Information Services (OGIS) on two training sessions:
 - FOIA Public Liaison Training for the DHS FOIA Public Liaisons
 - Dispute Resolution Skills for FOIA Professionals
- Trained staff on recent rulings in FOIA and Privacy Act cases.
- Collaborated with the ICE Chief FOIA Officer to provide an overview of the Alien File and Exemption 7, including practical application for DHS records.
- Collaborated with the FEMA Chief FOIA Officer to train staff on Exemption 4, including practical application for DHS records.
- Partnered with CRCL's FOIA Officer, Programs Branch Director, Compliance Branch Director and Deputy Director to train on CRCL's mission and structure, and the types of records under its purview.



Reporting

The Privacy Office issues the following public reports, including this one, that document progress in implementing DHS privacy and FOIA policy. All reports can be found on the Privacy Office website under Privacy Results and Reports: www.dhs.gov/privacy.

- ***Privacy Office Semi-Annual Section 803 Report to Congress:*** The Privacy Office issues two semi-annual reports to Congress as required by Section 803 of the 9/11 Commission Act,¹⁹ as amended. These reports include: (1) the number and types of privacy reviews undertaken by the CPO; (2) the type of advice provided and the response given to such advice; (3) the number and nature of privacy complaints received by the Department; and (4) a summary of the disposition of such complaints and the reviews and inquiries conducted. In addition, the Privacy Office provides statistics on privacy training and awareness activities conducted by the Department.
- ***Annual FOIA Report to the Attorney General of the United States:*** This report provides a summary of Component-specific data on the number of FOIA requests received, the disposition of such requests, reasons for denial, appeals, response times, pending requests, processing costs and fees collected, and other statutorily required information.
- ***Chief Freedom of Information Act Officer Report to the Attorney General of the United States:*** This report discusses actions taken by the Department to apply the presumption of openness and to ensure that DHS has an effective system to respond to requests, increase proactive disclosures, fully utilize technology, reduce backlogs, and improve response times.
- ***DHS Data Mining Report to Congress:*** This report describes DHS activities already deployed or under development that fall within the Federal Agency Data Mining Reporting Act of 2007²⁰ definition of data mining.
- ***Social Security Number Fraud Prevention Act Report to Congress:*** This report documents the Privacy Office's plan to reduce the collection, use, and mailing of Social Security numbers at DHS.
- ***Privacy and Civil Liberties Assessment Reports:*** [Executive Order 13636](#) (EO 13636), *Improving Critical Infrastructure Cybersecurity*, and [Executive Order 13691](#) (EO 13691), *Promoting Private Sector Cybersecurity Information Sharing*, require that senior agency officials for privacy and civil liberties assess the privacy and civil liberties impacts of the activities their respective departments and agencies have undertaken to implement the Executive Orders, and to publish their assessments annually in a report compiled by the Privacy Office and CRCL.

¹⁹ Pursuant to the *Intelligence Authorization Act for Fiscal Year 2014*, Pub. L. No. 113-126 (July 7, 2014), the reporting period was changed from quarterly to semiannually. The Privacy Office semiannual reports cover the following time periods: April – September and October – March.

²⁰ 42 U.S.C. § 2000ee-3.



III. Compliance & Oversight

The Privacy Office's FY 2015-2018 Strategic Plan includes four strategic goals:

Goal Three (Compliance and Oversight):

- *Conduct robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all DHS activities,*
- *Promote privacy best practices and guidance to the Department's information sharing and intelligence activities, and*
- *Ensure that privacy incidents and complaints are reported systematically, processed efficiently, and mitigated appropriately in accordance with federal and DHS privacy policies and procedures.*

In addressing new risks or adopting new and integrated approaches to protecting individual privacy, the privacy enterprise must anticipate any potential for infringement of core privacy values and protections, and address that risk accordingly. When issues are identified and resolved early, it helps ensure that programs and services provide the maximum public benefit with the lowest possible privacy risk.

Privacy Compliance

The Privacy Office ensures that privacy protections are built into Department systems, initiatives, projects, and programs as they are developed and modified, working with program or system owners and mission stakeholders across DHS during all phases of their projects. We assess the privacy risk of Departmental programs and develop mitigation strategies by reviewing and approving all DHS privacy compliance documentation.

The DHS privacy compliance documentation process²¹ includes four primary documents: PTA, PIA, SORN, and, when applicable, the PCR. PIAs assess risk by applying the universally recognized FIPPs to Department programs, systems, initiatives, and rulemakings. Each of these documents has a distinct function in implementing privacy policy at DHS, but together they enhance the transparency of Department activities and demonstrate accountability. Our compliance document templates and guidance are recognized Government-wide as best practices, and used by other Government agencies. See Appendix C for a detailed description of the compliance process and documents.

The Privacy Office also conducts privacy reviews of OMB Exhibit 300 budget submissions, and supports Component privacy officers and PPOCs to ensure that privacy compliance requirements are met. The Privacy Office is responsible for ensuring that the Department meets statutory requirements such as Federal Information Security Modernization Act of 2014 (FISMA)²² privacy reporting.

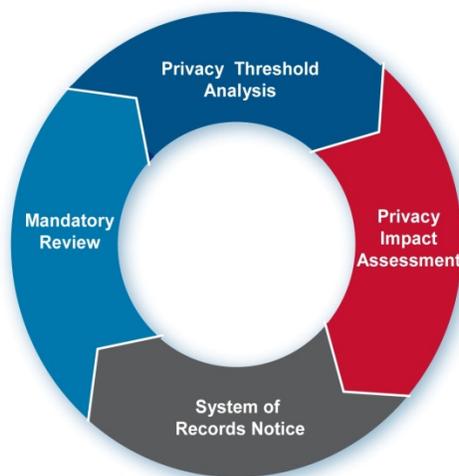


Figure 4: Privacy Office Compliance Process

²¹ See Appendix C for a description of privacy compliance documentation.

²² 44 U.S.C. Chapter 35 (44 U.S.C. §§ 3551-3558). See 44 U.S.C. § 3554, Federal agency responsibilities, for agency reporting requirements.

-
- At the end of June 2018, the Department’s FISMA privacy score showed that 97 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 100 percent of required SORNs have been completed.
 - Since 2015, no new Authorities to Operate can be granted for IT systems without the CPO’s approval.

Privacy Impact Assessments

The Privacy Office publishes new and updated PIAs on its website: www.dhs.gov/privacy. During the reporting period, the CPO approved 69 PIAs. A complete list by Component can be found in Appendix D.

Listed here are 19 key PIAs approved during this reporting period:

1. [DHS/ALL/PIA-063 Drug-Free Workplace Program](#)

Background: The Federal Drug-Free Workplace Program was established by Executive Order (EO) 12564 on September 15, 1986, to address illegal drug use by federal employees. The DHS Office of the Chief Human Capital Officer (OCHCO) oversees the departmental Drug-Free Workplace (DFW) program, and developed and implemented a comprehensive DFW program that includes the Components developing their own DFW plans that conform to DHS policies.

Purpose: DHS conducted this PIA to outline the collection and use of the PII of current employees and applicants who are selected for employment at DHS and subject to the requirements of the DHS DFW program. (*January 2, 2018*)

2. [DHS/ALL/PIA-066 DHS Employee Assistance Program \(EAP\)](#)

Background: Each Federal Executive Branch agency is required to have an Employee Assistance Program (EAP), which is a voluntary, confidential program that helps employees and their family members work through various life challenges that may adversely affect job performance, health, and personal well-being. DHS EAP services include assessment, counseling, and referrals for employees and family members with personal or work-related concerns such as job stress, financial issues, legal matters, family problems, office conflicts, and alcohol and substance abuse disorders. EAP assistance may be sought by the employee, by a family member, or at the recommendation of an employee’s supervisor.

Purpose: DHS conducted this PIA as DHS EAP service providers collect PII about individuals who receive assistance through the program. (*June 11, 2018*)

3. [DHS/ALL/PIA-052\(a\) DHS Insider Threat Program](#)

Background: The DHS Insider Threat Program (ITP) was established as a department-wide effort to manage insider threat matters within DHS. The Insider Threat Program was mandated by E.O. 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,” issued October 7, 2011. This

EO requires all federal agencies that operate or access classified computer networks, to establish an insider threat detection and prevention program covering all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government), to ensure the security of classified networks and the responsible sharing and safeguarding of classified information on those networks with appropriate protections for privacy and civil liberties. Insider threats include: attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against the Department and its personnel, facilities, resources, and activities; unauthorized use of or intrusion into automated information systems; unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary information or technology; and indicators of potential insider threats. The DHS ITP monitors activity on all three DHS networks: Unclassified (A-LAN), SECRET (B-LAN also known as the Homeland Secure Data Network), and TOP SECRET (C-LAN also known as the Joint Worldwide Intelligence Communications System) for activities that would qualify as an insider threat.

Purpose: DHS updated this PIA to reflect the application of the insider threat program to all networks. (*March 1, 2018*)

4. [DHS/ALL/PIA-064 Preventing and Combating Serious Crime \(PCSC\) Agreements - Greece and Italy](#)

Background: In 2009, the United States entered into two separate *Enhancing Cooperation in Preventing and Combating Serious Crime Agreements* (PCSC Agreements) with the Hellenic Republic (Greece) and the Italian Republic (Italy). PCSC Agreements permit the United States and its partner countries to cooperatively exchange biometric and biographic data in the course of preventing and combating serious crimes and terrorist activities. DHS owns and maintains the Automated Biometric Identification System (IDENT), which is responsible for processing automated fingerprint queries to determine if a person of interest encountered by a partner country has also been encountered by DHS. While existing PCSC agreements between DHS and its partners allow for the exchange of criminal justice data, the agreements with Greece and Italy also enable DHS to share non-criminal justice data from USCIS.

Purpose: The Privacy Office published this PIA to identify risks and mitigations associated with this information sharing, and to discuss the legal and policy justifications for sharing non-criminal justice data from the USCIS with Greece and Italy under the respective PCSC Agreements, for purposes of immigration vetting and criminal justice, including border enforcement processes. (*April 3, 2018*)

5. [DHS/CBP/PIA-044 Joint Integrity Case Management System \(JICMS\)](#)

Background: The Joint Integrity Case Management System (JICMS) records claims of employee misconduct, manages criminal and administrative investigations, and tracks employee and contractor disciplinary actions. The CBP and ICE Offices of Professional Responsibility are responsible for the overall operation of JICMS, however other DHS components may use JICMS for their internal affairs case management. (*July 18, 2017*)

Purpose: CBP published this PIA to assess the privacy risks and mitigations associated with JICMS because it collects, stores, and uses PII about DHS employees, contractors, and members of the public.

6. [DHS/CBP/ PIA-030\(d\) Traveler Verification Service \(TVS\): CBP-TSA Technical Demonstration](#)

Background: CBP is continuing to develop and expand its biometric entry-exit system for international flights at airports throughout the United States. In partnership with the TSA, CBP's latest biometric technical demonstration will use the Traveler Verification Service (TVS) cloud-based matching service to compare international travelers' photos captured by CBP against previously captured photos.

Purpose: CBP updated this PIA to provide the public with notice regarding CBP's plans to use PII collected by CBP devices located at TSA security checkpoints. *(September 25, 2017)*

7. [DHS/CBP/ PIA-049 CBP License Plate Reader Technology](#)

Background: CBP uses a combination of surveillance systems, including license plate reader technology, to provide comprehensive situational awareness along the United States border to assist CBP in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law. License plate reader technology includes commercially available technologies such as fixed and mobile license plate readers.

Purpose: CBP conducted this PIA to provide public notice of this CBP-owned and operated technology, assess the privacy risks, and describe the steps CBP is taking to mitigate them. *(December 11, 2017)*

8. [DHS/CBP/PIA-008\(a\) Border Searches of Electronic Devices](#)

Background: CBP updated this PIA to provide notice and a privacy risk assessment of the CBP policy and procedures for conducting searches of electronic devices pursuant to its border search authority.

Purpose: CBP updated this PIA to describe recent changes to, and the reissuance of, CBP's policy directive governing border searches of electronic devices, [CBP Directive No. 3340-049A, Border Searches of Electronic Devices \(January 2018\)](#). CBP also conducted a privacy risk assessment of this updated policy as applied to any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones and other communication devices, cameras, and music and other media players. Noting the evolution of the operating environment since the 2009 Directive was issued, along with advances in technology and other continuing developments, CBP reviewed and updated its Directive. *(January 4, 2018)*

9. [DHS/CBP/PIA-051 Automated Passport Control \(APC\)/Mobile Passport Control \(MPC\)](#)

Background: The Automated Passport Control (APC) and Mobile Passport Control (MPC) programs automate and expedite eligible travelers' entry process into the United States. These programs enable travelers to perform select entry declaration and inspection requirements tasks through a self-service kiosk (APC) or a mobile device application (MPC).

Purpose: CBP published this PIA as APC and MPC collects PII from members of the public. (March 19, 2018)

10. [DHS/FEMA/PIA-040\(a\) Deployment Tracking System](#)

Background: FEMA's Office of Response and Recovery (ORR), Field Operations Directorate, Workforce Management Division (WMD) coordinates personnel deployment programs under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act). The WMD Deployment and Analysis Branch operates the Deployment Tracking System (DTS) to assign and track the deployment of disaster response and recovery personnel.

Purpose: FEMA conducted this PIA because FEMA collects, uses, maintains, retrieves, and disseminates PII in DTS to coordinate and manage the deployment of federal emergency response and recovery personnel to federally-declared emergencies and disasters. This PIA updates and supersedes the previously published DTS Beta Test PIA. (July 19, 2017)

11. [DHS/FEMA/PIA-049 Individual Assistance \(IA\) Program](#)

Background: The FEMA Office of Response and Recovery (ORR), Individual Assistance Division manages the Individual Assistance (IA) programs. These programs provide disaster recovery assistance to individuals and support FEMA's recovery mission under the Stafford Act through the collection and processing of disaster survivor information obtained through electronic or paper-based means.

Purpose: FEMA published this PIA to broadly cover the collection, use, maintenance, retrieval, and dissemination of PII of applicants to implement the FEMA IA programs. (January 11, 2018)

12. [DHS/ICE/PIA-039 Acquisition and Use of License Plate Reader Data from a Commercial Service](#)

Background: ICE procured query-based access to a vendor-owned commercial License Plate Reader (LPR) data service that stores recorded vehicle license plate data from cameras equipped with license plate reader technology. ICE uses LPR data from this service in support of its criminal and administrative law enforcement missions. In March 2015, ICE published a PIA announcing ICE's intention to procure access to a commercial LPR database and describing the controls ICE would put in place to ensure the agency complies with privacy and civil liberties requirements when using the service.

Purpose: ICE updated this PIA to explain ICE’s operational use of the service it has procured and describes the privacy and civil liberties protections that have been implemented by the agency and the vendor. *(December 27, 2017)*

13. DHS/NPPD/PIA-020(b) Private Sector Clearance Program for Critical Infrastructure

Background: NPPD updated the Private Sector Clearance Program for Critical Infrastructure’s (PSCP) PIA to account for changes to the PSCP clearance process and to the DHS Form 9014, Private Sector Clearance Request Form.

Purpose: NPPD updated and replaced the previous PIA, last published in March 2018, to remove references to the Cooperative Research and Development Agreement and the Classified Critical Infrastructure Protection Program because such references were also removed from the newly renamed DHS Form 9014, Private Sector Clearance Request Form. *(April 20, 2018)*

14. DHS/TSA/PIA-046 Travel Document Checker Automation Using Facial Recognition

Background: TSA conducted a three-week proof of concept at Los Angeles International Airport for automating the identity verification portion of the Travel Document Checker (TDC) process using facial recognition technology. TSA tested the use of a National Institute for Standards and Technology (NIST)-compliant facial matching algorithm to compare the facial images of aviation passengers who were e-Passport holders on outward-bound international flights and who voluntarily entered the screening checkpoint through automated electronic security gates or “e-Gate.” The e-Gate device captures an image of the passenger’s face and compares it to the biometric image in the passenger’s e-Passport. The e-Gate attempts to replicate the function of the TDC and authenticate the passenger’s e-Passport and boarding pass. The operational goals of this proof of concept was to assess critical operational and technological components of the e-Gate, including the viability of using facial recognition technology for identity verification, and to capture specific metrics to inform future requirements for improving the security and speed of identity verification at airport checkpoints.

Purpose: TSA published this PIA to address the privacy risks inherent in the use of facial recognition technology during the proof of concept. *(January 5, 2018)*

15. DHS/USCG/PIA-026 USCG Research and Development Center (RDC) Small Unmanned Aircraft Systems (sUAS) Program

Background: The USCG Research and Development Center (RDC) was tasked and funded to evaluate small Unmanned Aircraft Systems (sUAS) for potential use by USCG for operational missions. sUAS include small aircrafts (typically less than 55 pounds in weight) that are generally operated using a wireless ground control station (GCS). The aircrafts are equipped with sensors and cameras that can capture images and transmit them to standalone GCSs to provide aerial views of USCG missions for situational awareness to the operators and users.

Purpose: USCG conducted this PIA to address the privacy impacts of sUAS surveillance and image capturing capabilities. *February 22, 2018)*

16. [DHS/USCIS/PIA-068 Refugee Case Processing and Security Vetting](#)

Background: USCIS and the Department of State (DOS) work cooperatively to administer the overseas component of the U.S. Refugee Admissions Program (USRAP). The mission of the USRAP is to resettle eligible refugees in the United States. Although DOS has overall management responsibility for the USRAP, USCIS Refugee, Asylum, and International Operations Directorate (RAIO) Refugee Affairs Division (RAD), and in some cases International Operations (IO) Division, is responsible for interviewing refugee applicants, receiving and reviewing results of all background checks, and adjudicating applications for refugee status.

Purpose: USCIS published this PIA because the USRAP collects, uses, and maintains PII in support of refugee resettlement and employment eligibility. This PIA comprehensively covers current USRAP processes and procedures. USCIS will update and republish this PIA immediately should the USRAP vetting process change. (*July 21, 2017*)

17. [DHS/USCIS/PIA-027\(c\) Asylum Division](#)

Background: The Asylum Division of USCIS adjudicates applications for asylum benefits pursuant to Section 203 of the Nicaraguan Adjustment and Central American Relief Act (NACARA § 203); withholding of removal under the terms of a settlement agreement reached in a class action; and screening determinations for safe third country, credible fear, and reasonable fear. The Asylum Division maintains the Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS). Both systems, originally developed by the former Immigration and Naturalization Service (INS), are used by the USCIS Asylum Division to capture information pertaining to asylum applications, credible fear and reasonable fear screening processes, and applications for benefits provided by NACARA § 203.

Purpose: USCIS updated and reissued this PIA because the Asylum Division manages records and systems containing PII in order to conduct its adjudications. (*July 21, 2017*)

18. [DHS/USSS/PIA-020 United States Secret Service Counter Surveillance Division Unmanned Aircraft Systems Program Test](#)

Background: The USSS Counter Surveillance Division (CSD) conducted a Proof of Concept to test and evaluate a tethered small Unmanned Aircraft System (sUAS) during a Presidential visit to the Trump National Golf Club in Bedminster, New Jersey, in August 2017. The Proof of Concept helped determine the potential future use of tethered sUAS in supporting the Agency's protective mission. The tethered sUAS used in the Proof of Concept operated using a microfilament tether that provides power to the aircraft and the secure video from the aircraft to the Operator Control Unit (OCU). The sUAS was equipped with electro-optical and infrared (IR) camera.

Purpose: The USSS conducted this PIA to evaluate the privacy risks associated with tethered sUAS's surveillance and image capturing capabilities. This PIA is limited to covering the use of electro-optical and IR sensors on a single tethered sUAS during one event. Any other use of

these types of sensors by USSS on USSS aircraft—including sUAS—will be addressed in a future PIA. *(August 2, 2017)*

19. DHS/ USSS/PIA-021 Comprehensive Incident Database on Targeted Violence (CID-TV)

Background: The USSS Comprehensive Incident Database on Targeted Violence (CID-TV) is an on-going research project that analyzes past incidents of targeted violence directed toward public officials, public figures, and prominent facilities, structures, or events in support of the mission of the National Threat Assessment Center (NTAC), Office of Strategic Intelligence and Information (SII).

Purpose: The USSS published this PIA to evaluate the privacy risks associated with CID-TV collecting PII. *(May 4, 2018)*

System of Records Notices

The Privacy Office publishes new and updated SORNs on its website: www.dhs.gov/privacy. During the reporting period, the CPO approved 14 SORNs and three were rescinded. A complete list by Component can be found in Appendix D.

Listed here are five key SORNs approved during this reporting period:

1. [DHS/ALL-040 DHS Personnel Recovery Information System of Records](#)

Background: The DHS Personnel Recovery Programs are responsible for: ensuring that DHS personnel and contractors assigned overseas or on official travel outside the continental United States have proper training and equipment to fulfill their respective mission; maintaining a twenty-four (24) hour monitoring center for all overseas personnel who are traveling outside their country of assignment; executing a coordinated response to personnel recovery incidents; maintaining a notification system within DHS to provide emergency-related notifications as needed without jeopardizing the safety of DHS personnel (including federal employees and contractors); and providing and developing tracking and locating technology.

Purpose: The purpose of this system is to permit DHS's collection, use, maintenance, dissemination, and storage of information to: facilitate identification of DHS personnel (including employees and contractors) assigned overseas or on official travel abroad for whom DHS has the responsibility to recover or account; maintain situational awareness of the location of DHS personnel; and coordinate support services for personnel who have been abducted, detained, held hostage, declared missing, impacted by a terrorist attack, natural disaster, government takeover, aircraft/motor vehicle accident, or are otherwise isolated from friendly support. (*October 25, 2017, 82 FR 49407*)

2. [DHS/ALL-041 External Biometric Records \(EBR\) System of Records](#)

Background: This system of records allows DHS to receive, maintain, and disseminate biometric and associated biographic information from non-DHS entities, both foreign and domestic, for the following purposes pursuant to formal or informal information sharing agreements or arrangements ("external information"), or with the express approval of the entity from which the Department received biometric and associated biographic information: law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities.

Purpose: The purpose of this system is to process and maintain biometric and associated biographic information from non-DHS entities, both foreign and domestic, for law enforcement, national security, immigration screening, border enforcement, intelligence, national defense, and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities. DHS may use and share these external biometric and associated biographic records for these same purposes, as permitted and approved by our partners, if applicable, pursuant to the agreement or arrangement. (*April 24, 2018, 83 FR 17829*)

3. [DHS/ICE-013 Alien Health Records System](#)

Background: This system of records allows the Department to maintain records that document the health screening, examination, and treatment of aliens arrested by the Department and detained by ICE for civil immigration purposes in facilities where the ICE Health Service Corps (IHSC) provides or oversees the provision of care.

Purpose: The purpose of this system is to document and facilitate the provision of medical, dental, and mental health care to individuals in ICE custody in facilities where care is provided by IHSC. The system also supports the collection, maintenance, and sharing of medical information for these individuals in the interest of public health, especially in the event of a public health emergency, such as an epidemic or pandemic. Finally, this system facilitates continuity of care after individuals are discharged from ICE facilities by providing individuals with direct access to their records and disclosing records to other parties (e.g., medical providers), as appropriate. The purpose of this system is also being updated to include the new IHSC Patient Medical Record Portal (the “Portal”), whereby individuals discharged from ICE facilities (either released from custody or removed from the United States) can log in and get a copy of their electronic medical record. As a result, a new category of records is being maintained in this system of records to support login capability for the Patient Medical Record Portal. (*March 19, 2018, 83 FR 12015*)

4. [DHS/USCG-029 Notice of Arrival and Departure \(NOAD\) System of Records](#)

Background: This system of records allows the USCG to facilitate the effective and efficient entry and departure of vessels into and from the United States, and assist with assigning priorities for complying with maritime safety and security regulations. As part of the Department’s ongoing effort to promote transparency regarding its collection of information, the Coast Guard is updating its November 2015 system of records notice to explain its changes to the routine uses. Additional updates to this notice were explained in the November 2015 update. Further, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

Purpose: The purpose of this system is to maintain NOAD information to improve navigation safety, enhance the Coast Guard’s ability to identify and track vessels, and heighten the Coast Guard’s overall situational and maritime domain awareness, which will enhance mariners’ navigation safety and the USCG’s ability to address threats to maritime transportation security. (*July 17, 2017, 82 FR 32715*)

5. [DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records](#)

Background: This system of records contains information regarding transactions involving an individual as he or she passes through the U.S. immigration process, some of which may also be covered by separate Systems of Records Notices. DHS primarily maintains information relating to the adjudication of benefits, investigation of immigration violations, and enforcement actions in Alien Files (A-Files). Alien Files became the official file for all immigration records created

or consolidated since April 1, 1944. Before A-Files, many individuals had more than one file with the agency. To streamline immigration recordkeeping, legacy Immigration and Naturalization Service issued each individual an Alien Number, allowing the agency to create a single file for each individual containing that individual's official immigration record. DHS also uses other immigration files to support administrative, fiscal, and legal needs.

Purpose: The purpose of this system of records is to facilitate administration of benefits and enforcement of provisions under the INA and related immigration statutes. A-Files (whether paper or electronic), immigration case files, Central Index System, Microfilm Digitization Application System, and the National File Tracking System are used primarily by DHS employees for immigration processing and adjudication, protection of national security, and administering and enforcing immigration and nationality laws and related regulations and policy. These records also assist DHS with detecting violations of immigration and nationality laws; supporting the referral of such violations for prosecution or other appropriate enforcement action; supporting law enforcement efforts and inspection processes at the U.S. borders; as well as to carry out DHS enforcement, immigration, intelligence, and or other homeland security functions. (*September 18, 2017, 82 FR 43556*)

Privacy Compliance Reviews

The Privacy Office exercises its oversight function under Section 222 of the Homeland Security Act to ensure that the Department's use of technology sustains and does not erode privacy protections,²³ primarily by conducting Privacy Compliance Reviews (PCR).²⁴ PCRs are a *constructive and collaborative* mechanism to assess implementation of protections described in PIAs, SORNs, or ISAAs, to identify areas for improvement, and to correct course if necessary. PCRs are distinct from the CPO's investigative authority.



The PCR framework emphasizes program involvement throughout the process in order to build trust with affected systems or programs. The outcomes and benefits of a PCR include early issue identification and remediation, lessons learned, recommendations, updates to privacy compliance documentation, and heightened awareness of privacy. PCRs are conducted in a collaborative setting with participants from the Privacy Office, Component Privacy Officers, and participants from affected programs.

PCRs may result in public reports or internal recommendations, depending upon the Chief Privacy Officer's objective for the review. Public PCR reports are available on the Privacy Office website: www.dhs.gov/privacy, under "Privacy Oversight."

During the reporting period, the Privacy Office completed three PCRs and continued to work on one PCR, oversaw implementation of recommendations from six previous PCRs, and launched one new PCR.

Mission cross-cutting goal: To mature and strengthen homeland security by preserving privacy, oversight, and transparency in the execution of all departmental activities.

²³ 6 U.S.C. § 142(a)(1).

²⁴ [DHS Privacy Policy Instruction 047-01-004](#) for PCRs on January 19, 2017.

PCRs Completed or Underway

[USCIS Customer Profile Management Service and National Appointment Scheduling System, October 16, 2017](#)

USCIS oversees lawful immigration to the United States. As part of this mission, USCIS receives and adjudicates requests for immigration and citizenship benefits. The administration of these benefits requires the collection of biographic and biometric information from benefits requestors. USCIS uses multiple systems to administer immigration benefits, including the Customer Profile Management Service (CPMS) and National Appointment Scheduling System (NASS). Due to the heightened privacy risks associated with the collection of biometric information, PIAs for CPMS and NASS in 2015 required the Privacy Office to conduct a PCR. During the course of this PCR, the Privacy Office found USCIS to be in compliance with federal privacy laws, DHS and Component privacy regulations and policies, and explicit assurances made by USCIS in existing privacy compliance documentation. The Privacy Office identified six recommendations designed to improve USCIS privacy compliance, and to incorporate best practices for other USCIS and DHS programs and systems.

[U.S. Customs and Border Protection's \(CBP\) Electronic System for Travel Authorization \(ESTA\), October 27, 2017](#)

CBP's use of social media identifiers to vet ESTA applications is defined in the September 2016 update to the ESTA PIA (DHS/CBP/PIA-007(g)). In September 2016, CBP began collecting, on a voluntary basis, social media identifiers from citizens and nationals of countries participating in the Visa Waiver Program who sought to travel to the United States. The inclusion of social media identifiers on the ESTA application is the first time DHS has requested social media information as part of an application for benefits or travel to the United States. In completing the PCR, the DHS Privacy Office found the CBP ESTA program's use of social media identifiers is compliant with the requirements outlined in the PIA and made three recommendations to enhance privacy best practices.

[National Operations Center Publicly Available Social Media Monitoring and Situational Awareness Initiative, December 8, 2017](#)

PCRs are a key aspect of the layered privacy protections built into the DHS National Operations Center's Media Monitoring Initiative to ensure that the protections described in the PIAs are followed. The Privacy Office conducted this eighth PCR to assess compliance with DHS privacy policy and the publicly available Social Media Monitoring and Situational Awareness Initiative PIA and SORN, as well as implementation of recommendations from previous PCRs. The Privacy Office found that the DHS Office of Operations Coordination, National Operations Center, continues to comply with the privacy requirements identified in privacy compliance documents, and made five recommendations to further improve privacy protections.

PCRs with Ongoing Oversight

[Office of the Chief Human Capital Officer – Completed September 30, 2015 with ongoing oversight](#)

The Privacy Office conducted a PCR of the Office of the Chief Human Capital Officer (OCHCO) in 2015 based on *DHS Privacy Policy Directive 140-06*, which included 25 recommendations to improve the culture of privacy at OCHCO. The recommendations focused on the areas of transparency/awareness, data minimization/retention limits, use limitations, data integrity, data security, and accountability.

Since publishing the 2015 PCR findings, OCHCO has had significant employee turnover with privacy responsibilities, and the Privacy Office has met numerous times with the Chief Human Capital Officer and OCHCO staff to encourage implementation of the recommendations, focusing on how OCHCO will make sustainable plans and actions to promote culture change. The Privacy Office continues to seek more robust privacy practices and greater privacy awareness among OCHCO personnel, especially given their day-to-day work with PII. OCHCO submitted implementation status reports in September 2017 and June 2018 in compliance with the 2015 PCR biannual self-audit requirement.

[U.S. – European Union \(EU\) Passenger Name Records Agreement – Completed July 2, 2015 with ongoing oversight](#)

The June 26, 2015 PCR informed discussions during a joint review of the 2011 U.S. – EU Passenger Name Record (PNR) Agreement with the European Commission on July 1-2, 2015. During the joint review, DHS thoroughly explained its use and protection of PNR, and presented its compliance with the terms of the 2011 Agreement. On January 19, 2017, the European Commission published its conclusions from the joint review, which found that DHS continues to comply with the conditions in the Agreement.

The Privacy Office led monthly PNR privacy working group meetings throughout the reporting period to monitor implementation of the 2015 PCR's 12 recommendations, as well as the 10 recommendations from the European Commission's January 2017 report. Throughout this time, the Privacy Office found DHS stakeholders to be careful stewards of the data, faithfully following stated PNR policies and practices, and fully complying with the terms of the Agreement.

[Analytical Framework for Intelligence, December 6, 2016](#)

CBP's Analytical Framework for Intelligence (AFI) is an analyst-oriented, web-based application that augments CBP's ability to gather and develop information about persons, events, and cargo of interest by enhancing search and analytical capabilities of existing data systems. On December 6, 2016, the Privacy Office finalized its second PCR of AFI that found that CBP continues to operate and manage AFI with privacy-protective objectives, and with sensitivity to privacy and data aggregation risks. The Privacy Office recommended that CBP implement eight additional recommendations to continue to improve its ability to demonstrate compliance with privacy requirements, and required implementation status updates of the recommendations regularly thereafter. CBP provided its first implementation status report, to which, on October

23, 2017, the Privacy Office considered four of the recommendations to be fully implemented. The Privacy Office requested another status report that is pending at this time.

[Southwest Border Pedestrian Exit Field Test, December 30, 2016](#)

CBP conducted the Southwest Border Pedestrian Exit Field Test (test) to determine whether the collection of biometric information, including facial and iris images, from visitors exiting the United States enhances CBP exit operations with acceptable impacts to the public's travel experience and border processing times. Specifically, this test evaluated whether the processes and technologies used to collect biometric information would enable CBP to more effectively identify individuals who have overstayed their period of admission, identify individuals who pose a law enforcement or national security threat, and improve CBP reporting and analysis of all travelers entering and exiting the United States.

The Privacy Office completed its PCR of the test in December 2016 that found that CBP managed this test with privacy-protective objectives and with sensitivity to privacy and data aggregation risks, making 10 best practice recommendations for any future biometric exit tests to further improve its ability to demonstrate compliance with privacy requirements. CBP provided its first implementation status report on October 23, 2017; the Privacy Office considered all of the recommendations to be fully implemented. No further reporting is required.

Nationwide Suspicious Activity Reporting (SAR) Initiative,²⁵ December 11, 2017

The Nationwide SAR Initiative (NSI) is designed to facilitate the sharing of suspicious activities information between DHS, the Federal Bureau of Investigation (FBI), and federal, state, local, and tribal law enforcement entities through the NSI SAR Data Repository (NSI SDR), which is held in the FBI's eGuardian system. "Suspicious activities" are defined by the Information Sharing Environment Functional Standard (hereinafter "Functional Standard") as "observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity." Following submission through the FBI's eGuardian platform, reports of suspicious activities meeting the Functional Standard are shared and stored in the NSI SDR as Information Sharing Environment-Suspicious Activity Reports (ISE-SAR).

A PCR, concluded in April 2017, resulted in recommendations and best practices to improve DHS Components' compliance with both NSI and DHS privacy requirements. In December 2017, the Privacy Office worked with the DHS NSI Program Management Office (PMO) to determine implementation of the recommendations and best practices. The Privacy Office reviewed Component Privacy Officers' audits of ISE-SARs submitted to the NSI SDR and determined there was appropriate oversight, with appropriate steps being taken if any non-compliant reports were found. During the normal compliance life cycle, some Components have updated their privacy compliance documents to ensure Functional Standard, privacy, civil rights, and civil liberties compliance. The Privacy Office continues to work with the NSI PMO to promote best practices, and with Components on their self-auditing efforts.

²⁵ This PCR is not posted on the DHS website.

[United States Secret Service \(USSS\), July 21, 2017](#)

On October 7, 2016, the DHS Office of Inspector General (OIG) issued report OIG-17-01, “[USSS Faces Challenges Protecting Sensitive Case Management Systems and Data](#)” that recommended that the DHS Privacy Office “conduct a systemic review with recommendations for ensuring USSS compliance with DHS privacy requirements.” The DHS Privacy Office concluded its PCR in July 2017 based on the OIG recommendation, which found that USSS requires significant resources to have an effective privacy program that incorporates robust outreach, collaboration, and oversight. The PCR made 12 recommendations for USSS to improve its privacy posture. The DHS Privacy Office met quarterly with the USSS Privacy Office during the reporting period and received a written report and supporting documentation on the implementation status of all recommendations in August 2018.

PCRs Launched or in Process

- On May 30, 2018, the Privacy Office launched a PCR to identify and mitigate risk that may be incurred by inadvertent disclosure of information protected by Title 8, United States Code, Section 1367, *Violence Against Women Act (VAWA)*, as well as T and U visa applicants. The PCR focuses on those Components and offices most likely to access or be responsible for dissemination of Section 1367 records: ICE, CBP, USCIS, OBIM, and I&A.
- The Privacy Office will soon finalize its review of the DHS Countering Violent Extremism Grant Program (CVEGP). Due to the complexity of the program’s management, the role of various Components, the Administration change that impacted the program’s awards, and staff changes within the Privacy Office, this PCR took longer than expected. The Privacy Office reviewed the programs’ degree of compliance with the [Office for Community Partnerships \(OCP\) CVEGP PIA](#) and [Privacy Policy Guidance Memoranda 2008-01/Privacy Policy Directive 140-06](#). A final product has not yet been determined.

Computer Matching Agreements

Under the *Computer Matching and Privacy Protection Act of 1988*, which amended the Privacy Act, federal agencies must establish a Data Integrity Board to oversee and approve their use of Computer Matching Agreements (CMA).²⁶ The CPO serves as the Chairperson of the DHS Data Integrity Board (DIB), and members include the Inspector General, the Officer for CRCL, the CIO, and representatives of Components that currently have an active CMA in place.²⁷

Before the Department can match its data with data held by another federal agency or state government, either as the recipient or as the source of the data, it must enter into a written CMA with the other party, which must be approved by the DIB. CMAs are required when there is a comparison of two or more automated systems of records for verifying the eligibility for cash or in-kind federal benefits.²⁸

CMAs benefit the public by ensuring that funding is not duplicated or erroneous, and protect the Sensitive PII of vulnerable populations, such as needy families, small business owners, student loan recipients, and natural disaster survivors. The DIB seeks to expose fraud and waste while ensuring that computer matching does not result in misuse or abuse of Sensitive PII (the latter concern prompted Congress to pass the Computer Matching and Privacy Protection Act). In November 2017, the Privacy Office issued a revised internal Standard Operating Procedure (SOP) on CMAs, templates for agreements with both federal and state agencies, and a detailed methodology for carrying out a Cost-Benefit Analysis.

Under the terms of the computer matching provisions of the Privacy Act, a CMA may be established for an initial term of 18 months. Provided there are no material changes to the matching program, existing CMAs may be re-certified once for a period of 12 months. Thus, the Department must re-evaluate the terms and conditions of long-standing computer matching programs regularly.

The DIB conducted its annual review of CMA activity on December 7, 2017. The Privacy Office subsequently submitted the Department's [Computer Matching Activity Annual Report](#) to OMB, covering Calendar Year 2017.

DHS continues to be party to 11 CMAs that can be found on the Privacy Office website.

²⁶ With certain exceptions, a matching program is “any computerized comparison of -- (i) two or more automated systems of records or a system of records with non-federal records for the purpose of (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under federal benefit programs. . . .” 5 U.S.C. § 552a(a)(8)(A)(i)(I).

²⁷ The Secretary of Homeland Security is required to appoint the Chairperson and other members of the Data Integrity Board. 5 U.S.C. § 552a(u)(2). The Inspector General is a statutory member of the Data Integrity Board. 5 U.S.C. § 552a(u)(2).

²⁸ 5 U.S.C. § 552a(o).

FOIA Compliance and Oversight

The Chief Privacy Officer is also the Chief FOIA Officer, and is responsible for the agency-wide compliance of the DHS FOIA Program in accordance with the [FOIA Compliance Policy Directive 262-11](#). Further, the [2016 FOIA Improvement Act](#) requires the Chief FOIA Officer to “...review, not less frequently than annually, all aspects...” of the agency's administration of the FOIA “...to ensure compliance...” with the FOIA requirements. This includes reviewing Agency regulations, disclosure of records under paragraphs (a)(2) and (a)(8), assessment of fees and fee waivers, timely processing of requests, use of exemptions, and dispute resolution services with the Office of Government Information Services (OGIS) or FOIA Public Liaisons.



As part of this compliance review, the Chief FOIA Officer disseminated the Department of Justice (DOJ) Self-Assessment Tool-Kit to Component FOIA Officers. The Self-Assessment Tool-Kit is comprised of 13 modules on a variety of FOIA functions. From the responses, the Chief FOIA Officer hopes to better understand the processes at each Component, and find areas in which the Privacy Office needs to focus on through training, support, and enhanced cross-Component consistency.

FOIA Operations:²⁹ DHS consistently receives the largest number of FOIA requests of any federal department or agency, receiving almost 40 percent of all requests within the Federal Government. This year's increase tracks with the increased public interest in the Department's operations, which includes the execution of Departmental priorities like the recent Presidential Executive Orders and guidance from the Secretary. In FY 2017, DHS received 366,036 requests, a 12 percent increase from the previous fiscal year, and responded to 367,546 requests, an 18 percent increase from the previous fiscal year. DHS released more than 32 million pages of records in response to FOIA requests, approximately 126,000 pages through the FOIA appeals process, and approximately 130,000 pages through FOIA litigation.

FOIA Backlog: In FY 2017, the Department decreased its backlog by six percent, from 46,788 requests in FY 2016 to 44,117 requests. This decrease is attributable to the concerted effort of the Privacy Office and our partner Components to address the Department's backlog.

- NPPD decreased its backlog by 93 percent, despite receiving 40 percent more requests in FY 2017.
- FEMA decreased its backlog by 79 percent by responding to 115 percent more requests in FY 2017.

²⁹ For efficiency, Departmental data reflects the reporting period used in the *Freedom of Information Act Annual Report*.

-
- CBP had a backlog of only about 1,000 requests, despite receiving 88,840 requests (a 33 percent increase) in FY 2017.

Backlog Reduction: Reducing the backlog is one of the Privacy Office's top priorities. The Privacy Office again collaborated with OBIM leadership in April 2017 to execute an aggressive backlog reduction. As a result, OBIM's backlog was reduced by over 99 percent by the end of FY 2017, from 13,000 requests to less than 40, thereby reducing the Department's backlog by 30 percent.

In addition, the Privacy Office determined that modernizing and consolidating FOIA IT systems into an enterprise-wide FOIA processing and case management system will create system efficiencies that could reduce the FOIA backlog and save money. To further this goal, the Privacy Office gained support from the former Deputy Secretary Elaine Duke, who approved a list of priority areas for budget and resource planning to address outdated IT systems in the Components, which included the FOIA IT systems. The Privacy Office is now leading an enterprise-wide FOIA Technology System Requirements Working Group to address outdated and duplicative FOIA IT Systems throughout DHS. In July 2018, the Working Group submitted a Capabilities Analysis Report to the Deputy Secretary's Management Action Group Joint Requirements Council that recommended scalable requirements for an enterprise-wide FOIA processing and case management system. A new, streamlined FOIA IT solution will save money, provide more consistent and accurate reporting on DHS programs and activities, satisfy regulations that require DHS to receive FOIA requests electronically through FOIA.gov, and allow DHS to move from paper-based to electronic processes.

Information Sharing and Intelligence Activities

The Privacy Office provides specialized expertise on information sharing agreements and programs to support the Department's information sharing activities with other federal agencies, the U.S. Intelligence Community, state and local entities, and international partners.

As mentioned earlier in this report, the work of the Privacy Office supports all five core DHS missions, as well as the important cross-cutting goal to *mature and strengthen homeland security by integrating information sharing and preserving privacy, oversight, and transparency in the execution of all departmental activities.*



There are currently more than 200 information-sharing agreements governing how DHS shares information. Requests for new agreements or amendments to existing agreements continue at a rapid pace. In accordance with numerous DHS Management Directives and Policy Instructions, the Privacy Office evaluates sharing requests that involve PII to mitigate privacy risks, incorporates privacy protections consistent with the DHS FIPPs, and audits or otherwise measures the effectiveness of those protections over time.

Data Access Review Council (DARC)

DARC is the coordinated oversight and compliance mechanism for the review of departmental initiatives involving the internal or external transfer of PII through bulk data transfers; these transfers support the Department's national and homeland security missions. The DARC advises on the challenges relating to bulk information sharing, including sharing in the cloud environment and application of advanced analytical tools to DHS data. The DARC ensures such transfers comply with applicable law and adequately protect the privacy, civil rights, and civil liberties of the individuals whose information is shared.

DARC initiatives primarily involve information sharing arrangements with members of the IC. DARC membership includes the Privacy Office, I&A, Office of Strategy, Policy, and Plans (PLCY), OGC, and CRCL.

During the reporting period, the Privacy Office worked with DHS stakeholders and IC partners to approve 45 ISAAs, or extensions for existing arrangements, and ensure identification and mitigation of privacy risks by completing privacy compliance documentation for these agreements. The Privacy Office also monitors reports generated in accordance with existing agreements' provisions to ensure general adherence to the terms, and to ensure appropriate reporting and mitigation of any privacy incidents involving DHS data. *Mission Number One: Prevent Terrorism and Enhance Security.*

Biometric Information Sharing

The Privacy Office continued to partner with the Policy Screening and Coordination Office and other Headquarters and Component biometric stakeholders to: (1) update and align high-level biometrics-based information sharing agreements with the Department of Defense and DOJ; and (2) offer advice on requirements for sharing consistent with DHS SORNs and DHS privacy policies. The Privacy Office also concurred on clearing specific information sharing projects with these agencies, providing expertise on the appropriate handling of biometric records being further ingested from the Department of Defense. These additional datasets provide access to Department of Defense regional command repositories, aiding DHS's border screening and vetting mission objective.



In addition, the Privacy Office became a member of the Homeland Advanced Recognition Technology (HART) Integrated Project Team (IPT). HART, the replacement enterprise biometric system for IDENT, provides DHS with a flexible, scalable, and efficient biometric data system with greater capacity, more functionality, multimodal storage, and enhanced capabilities. Through the IPT, the Privacy Office will review and address privacy and policy issues affecting HART planning, testing, implementation, and sustainment.

Intelligence Product Reviews

Since 2009, the Privacy Office has examined I&A's draft intelligence reports (FINTEL), raw intelligence information reports (IIR), and briefing materials, all of which are drafted to respond to immediate threats and planned intelligence requirements, and are intended for dissemination within and outside the Federal Government. In addition, the Privacy Office reviews requests for information (RFI) related to source development, non-bulk information sharing, and foreign disclosure. In conducting these reviews, the Privacy Office applies the Privacy Act of 1974, the DHS FIPPs, and other relevant privacy laws and policies to all materials under review.

The Privacy Office's product review function is an ongoing, real-time operational service for the Department, requiring round-the-clock monitoring of communications and quick response to I&A's requests for review of intelligence products. During this reporting period, the Privacy Office reviewed 294 IIRs and FINTEL, 35 briefing packages, and 347 RFI (at all levels of classification). The Privacy Office also reviewed I&A's standing information requirements to ensure that DHS did not solicit unauthorized or unneeded PII.

The Privacy Office, in cooperation with OGC's Intelligence Law Division and CRCL, is working closely with I&A to change the process from one of pre-publication review to post-production audit for FINTEL and IIRs. During the current reporting period, the Privacy Office audited a random sample of IIRs produced by one Component. This initial audit was intended to test audit processes and procedures and several lessons were learned that might make it feasible to implement IIR audits on a larger scale or with greater frequency. The Privacy Office anticipates being able to make the transition during the next reporting period. *Mission Number One: Prevent Terrorism and Enhance Security.*



- **New:** [Privacy Incident Responsibilities and Breach Response Team](#) establishes DHS policy, responsibilities, and requirements for responding to all incidents involving PII contained in DHS information; and establishes the requirement for the Chief Privacy Officer (CPO) to convene and lead a Breach Response Team when a “major incident” involving PII has occurred,³¹ or at the discretion of the CPO.
- **Revised:** [Privacy Incident Handling Guidance](#) (PIHG) establishes DHS policy for responding to privacy incidents by providing procedures to follow upon the detection or discovery of a suspected or confirmed incident involving PII in an unclassified environment.
- **Revised:** [Handbook for Safeguarding Sensitive PII](#) provides best practices and DHS policy requirements to prevent a privacy incident involving Sensitive PII during all stages of the information lifecycle: *when collecting, storing, using, disseminating, or disposing of Sensitive PII.*



Privacy Incident Tabletop Exercise

On April 10, 2018, the Privacy Office, in conjunction with FEMA’s National Exercise Division, sponsored the first Annual DHS Privacy Incident Tabletop Exercise in Washington, DC, with privacy representatives from all DHS Components in attendance. The tabletop exercise examined 1) key DHS decisions required to address a privacy incident; and 2) roles and responsibilities as outlined in the Privacy Incident Handling Guidance (PIHG).

The facilitated discussion focused on the following exercise-specific objectives:

1. Test the incident response plan through a simulation.
2. Refine and validate the incident response plan by identifying potential gaps or weaknesses in the incident response process at both the Component and enterprise levels.



³¹ A breach constitutes a “major incident” when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals’ PII constitutes a “major incident,” as defined in OMB M-18-02. The CPO, in coordination with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO), will first determine whether a privacy incident is considered a “major incident” that involves PII.

Incident Metrics

When a privacy incident is reported, the CPO, in consultation with the Component Privacy Officer and other appropriate parties, will determine if the incident is a minor or major incident based on the context of the incident and risks to the individuals and the DHS mission. The CPO is accountable for ensuring appropriate follow-up actions are taken, such as investigation and notification, and may delegate this responsibility to the affected Component.

During this reporting period, 710 confirmed privacy incidents were reported to the DHS SOC, a nine percent decrease from the last reporting period. Figure 5 shows the total number of both suspected and confirmed privacy incidents, broken down by Component.

Component	Suspected Incidents	Confirmed Incidents
CBP	42	18
HQ	23	15
FEMA	26	23
FLETC	5	2
ICE	66	65
NPPD	19	19
OIG	8	2
S&T	2	0
TSA	22	16
USCG*	58	76
USCIS*	525	530
USSS	3	0
Master ^{32*}	59	68
Total	858	834

Figure 5: Total number of suspected and confirmed privacy incidents by DHS Component for the time period July 1, 2017 – June 30, 2018

*The number of confirmed incidents is higher because the amount includes incidents opened prior to July 1, 2017 and confirmed after July 1, 2017.

Major Incident Involving DHS OIG Case Management System

In May 2017, a major privacy incident involving the DHS OIG Case Management System was detected. This incident affected approximately 246,167 Federal Government employees who were employed directly by DHS during 2012 through 2016. The compromised PII for these individuals included names, Social Security numbers, dates of birth, positions, grades, and duty stations. This information is used by the DHS OIG Office of Investigations to conduct identity confirmation during the complaint and investigative process.

³² A Master Incident occurs when multiple Components are involved in a single privacy incident.

Additionally, individuals associated with DHS OIG investigations from 2002 through 2014, which includes subjects, witnesses, and complainants, and who could be both DHS employees and non-DHS employees, were also part of the privacy incident scope. The PII contained in this compromised database varies for each individual depending on the documentation and evidence collected for a given case. Information contained in this database includes names, Social Security numbers, alien registration numbers, dates of birth, email addresses, phone numbers, addresses, and personal information provided in interviews with DHS OIG investigative agents.

After completing a comprehensive investigation and remediation, DHS issued notifications to and contracted with a third party vendor to provide identity protection services for a period of 18 months, at no cost, to affected individuals.

New Incident Reporting Web Portal

In September 2017, the Department launched a new enterprise-wide incident database, the Enterprise Cyber Operations Portal (ECOP). The Privacy Office worked with ECOP developers to include new privacy incident data fields outlined in OMB Memorandum M-17-12. The developers used the Privacy Office's Breach Response Roadmap to create a user-friendly portal and add new tracking, reporting, and analytical capabilities. To guarantee a successful transition, the Privacy Office led the meticulous and systematic transfer and close-out of all privacy incidents in the former EOOnline database.

In addition to the OMB required tracking data (total number of incidents by Department and per Component; total number of individuals affected), ECOP also provides data to facilitate trend spotting (to address under reporting and mis-reporting), and the task fields are set to prompt and assist Components in fulfilling their required incident reporting tasks in a timely manner. The Chief Privacy Officer can now choose to view specific dashboards, and readily assess privacy analyst and other stakeholder workflow progress.

The Privacy Office continues to work with the developers to improve ECOP's production, reporting, and tracking capabilities. Future enhancements will include new Component task checklists and spreadsheet capabilities.

Special Protected Classes – Unauthorized Disclosures

As previously mentioned in Chapter One, the confidentiality protections afforded to alien victims of crimes are statutorily required under Title 8, United States Code, Section 1367, *Violence Against Women Act* (herein Section 1367), as well as T and U visa applicants. The Officer for CRCL has, through Secretarial delegation, the authority to provide DHS-wide guidance and oversight on the implementation of Section 1367 confidentiality and prohibited source provisions. The Chief Privacy Officer must determine any potential impacts a privacy incident may have on the privacy of individuals, including those protected by Section 1367. Because of the shared responsibilities for ensuring the proper handling of Section 1367 information, in FY 2018 the Privacy Office and CRCL developed a process whereby the two offices share incidents of unauthorized Section 1367 disclosures. The two offices then work together to ensure all incidents are appropriately investigated, addressed, and resolved.

During the reporting period, the Privacy Office hosted two Special Protected Classes Unauthorized Disclosure forums to refresh and educate the PPOCs and Incident Practitioners. Section 1367 incident reporting has increased, which is a positive indicator that the department-wide outreach is taking effect. Of the 711 total confirmed privacy incidents during this reporting period, 13 relate to unauthorized disclosure of Section 1367 special protected class information. The team oversight approach produces effective solutions, and is proving to be a constructive mechanism overall.

Privacy Complaints

The Privacy Office is responsible for ensuring that the Department has procedures in place to receive, investigate, respond to, and, when appropriate, provide redress for privacy complaints. As required by Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007,³³ as amended, the Privacy Office is required to provide semi-annual reports to Congress with the number and nature of the complaints received by the Department for alleged violations; and a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of DHS's Chief Privacy Officer.³⁴ U.S. citizens, Lawful Permanent Residents, visitors to the United States, and aliens may submit privacy complaints to the Department.³⁵ The Privacy Office also reviews and responds to privacy complaints referred by employees throughout the Department, or submitted by other government agencies, the private sector, or the public. DHS Components manage and customize their privacy complaint handling processes to align with their specific missions, and to comply with Department complaint handling and reporting requirements.

The Privacy Office handles privacy complaints and inquiries submitted directly to it by Department employees, members of the public, and others. When a complaint raises a privacy issue involving a particular Component(s), the Privacy Office will refer it to the relevant Component Privacy Officer or PPOC and follow up as needed. The Privacy Office also addresses traveler complaints submitted through the Department's Traveler Redress Inquiry Program (DHS TRIP), specifically those submissions having a nexus to privacy, which, in the majority of instances, concern travelers' experience during screening or other interactions with Department personnel.³⁶ See the section below on Non-Privacy Act Redress Programs for more details.

³³ 42 U.S.C. § 2000ee-1(f).

³⁴ These semi-annual reports may be found here: <https://www.dhs.gov/publication/dhs-section-803-reports-congress/>.

³⁵ Any individual can submit a privacy complaint to the Department. However, any complaint that is considered a Privacy Act request pursuant to 5 U.S.C. § 552a and Department regulations, 6 C.F.R. Part 5, may only be processed by the Department if submitted by a U.S. citizen or lawful permanent resident, or by a covered person pursuant to the Judicial Redress Act (JRA), 5 U.S.C. § 552a, note. This is consistent with Department policy, specifically *DHS Privacy Policy Guidance Memorandum 2017-01, Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*. Section 14 of Executive Order 13768 restricted DHS's discretion to extend the rights and protections of the Privacy Act, subject to applicable law, beyond U.S. citizens and lawful permanent residents. The policy requires that DHS and Component decisions regarding the collection, maintenance, use, disclosure, retention, and disposal of information being held by DHS conform to an analysis consistent with the Fair Information Practice Principles (Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06). The policy is available at https://www.dhs.gov/sites/default/files/publications/PPGM%202017-01%20Signed_0.pdf.

³⁶ As required by the Privacy Office's Memorandum of Understanding with OIG, established due to Section 222 of the Homeland Security Act, we receive monthly reports of any privacy-related complaints received in by the OIG and their disposition of those complaints. OIG follows a similar process of referring complaints to relevant Components or to us, as appropriate. As a result of the Privacy Office's relationship with OIG, we also review draft OIG reports for privacy equities.

Between April 1, 2017 and March 31, 2018, the Department received 5,921 privacy complaints and closed 5,799. Figure 6 shows the categories and disposition of privacy complaints the Department received.

Type and Disposition of Privacy Complaints Received³⁷				
Type of Complaint	Number of complaints received during the reporting period	Disposition of Complaint		
		Closed, Responsive Action Taken	In Progress (Current Period)	In Progress (Prior Periods)
Process & Procedure	509	486	24	0
Redress	810	810	0	0
Operational	4375	4280	100	0
Referred	227	223	4	0
Total	5,921	5,799	128	0

*Figure 6: Privacy Complaints Received by DHS
April 1, 2017 – March 31, 2018*

³⁷ The totals include complaints from previous periods. The categories of complaints are defined in OMB M-08-21 and included in the Privacy Office's Section 803 Reports, available at <http://www.dhs.gov/publication/dhs-section-803-reports-congress>. For efficiency, the data reflects the reporting period used in the Section 803 Reports.

Privacy Act Amendment Requests

The *Privacy Act* permits an individual, as defined by the *Privacy Act* as a U.S. citizen or LPR, or defined as a covered person by the *Judicial Redress Act of 2015*, to request amendment of his or her own records.³⁸ As required by [DHS Privacy Policy Guidance Memorandum 2011-01, Privacy Act Amendment Requests](#) (Privacy Policy Directive 140-08), Component Privacy Officers and FOIA Officers are responsible for tracking all Privacy Act Amendment requests and reporting the disposition of those requests to the Privacy Office. The Privacy Office serves as the repository for those statistics.

Figure 7: Privacy Act Amendment Requests received by DHS during the reporting period by Component and disposition.

Privacy Act Amendment Requests July 2017 – June 2018				
Component	Received	Granted	Denied	Pending
CBP	4	2	1	1
ICE	2	0	2	0
USSS	1	0	0	1
TOTALS	7	2	3	2

³⁸ 5 U.S.C. § 552a(d)(2).

Non-Privacy Act Redress Programs

DHS also provides redress for individuals impacted by DHS programs through a number of other mechanisms that have a privacy nexus, including:

DHS Traveler Redress Inquiry Program (DHS TRIP).³⁹ DHS TRIP offers redress services to the public by providing a centralized processing point for individual travelers to submit redress inquiries. DHS TRIP was developed to assist individuals who believe they have been incorrectly denied boarding, identified for additional screening, or encounter problems at ports of entry into the country. During the reporting period, DHS TRIP received approximately 16,212 requests for redress, with an average response time (date case opened to date case closed) of approximately 36 days.

- The CPO is a member of the DHS TRIP Advisory Board, and the Privacy Office is an active DHS TRIP practitioner. The Privacy Office reviews redress inquiries alleging non-compliance with DHS privacy policy. In most cases, they are referred to the relevant Component to address.

OBIM Redress Program. OBIM maintains biometric information that is collected in support of DHS missions. One of the main goals of the redress program is to maintain and protect the integrity, accuracy, privacy, and security of the information in its systems.

- OBIM responded to seven redress requests during the reporting period.

Transportation Sector Threat Assessment and Credentialing Redress. TSA's Office of Intelligence and Analysis (OIA) conducts security threat assessments and completes adjudication services in support of TSA's mission to protect U.S. transportation systems from individuals who may pose a threat to transportation security. OIA provides daily checks on over 15 million transportation sector workers against the U.S. Government's Consolidated Terrorist Watchlist. OIA provides a redress process that includes both appeals and waivers for transportation sector workers who believe they were wrongly identified as individuals who pose a threat to transportation security. Typical redress requests have involved documentation missing from initial submissions, immigration issues, or requests for appeals and waivers for criminal histories.

- During the reporting period, OIA granted 5,337 appeals and denied 551.
- Additionally, OIA granted 2,375 waivers and denied 385.

³⁹ <https://www.dhs.gov/dhs-trip>



IV. Workforce Excellence

The Privacy Office’s FY 2015-2018 Strategic Plan includes four strategic goals:

Goal Four (Workforce Excellence): Develop and maintain the best privacy and disclosure professionals in the Federal Government.

The Privacy Office undertook several key initiatives during the reporting period to achieve this goal, including outreach, sponsoring leadership development opportunities, skills training, and tapping into new sources to recruit diverse talent.

Workforce

At the close of the reporting period, the Privacy Office had a total staff of 45: 33 federal employees, two detailees, and ten contractors, including the following back-filled positions:

- Senior Director for Information Sharing, Security, and Safeguarding
- Senior Director, FOIA Operations and Management
- Program Analyst (Privacy Compliance)
- Senior Privacy Analyst
- Government Information Specialists (FOIA)

Recruitment actions are underway to fill these vacant positions:

- Senior Director, Privacy Policy and Oversight
- Privacy Analysts (IS3)
- Privacy Analysts (Compliance)
- Information Technology Specialist (Privacy Policy and Oversight)
- Government Information Specialists (FOIA)

Budget

In FY 2017, the Privacy Office's enacted budget was \$7,851,000. The Privacy Office was able to maximize the effectiveness and efficiency of its funding by pursuing the following cost savings efforts:

1. Leveraged intra-agency agreements with Departmental offices and Components to reimburse the Privacy Office for infrastructure and license costs related to FOIAXpress, the web-based, commercial-off-the-shelf application used for processing FOIA and Privacy Act requests;
2. Collected almost \$472,400 in reimbursable funding, directing more resources toward privacy and FOIA support services contracts; and
3. Conducted a review of IT billing, data management and support requirements, resulting in an annual cost savings of \$245,000 for the Department.

Staff Training and Development

Privacy Office leadership is committed to employee professional growth and development, and encourages staff to take advantage of training and development opportunities. During the reporting period, more than 90 percent of staff either completed a training course or obtained certification in a job-related specialty. Employees have participated in highly competitive, rigorous, Department-sponsored leadership and professional development curriculums, such as the *DHS Senior Executive Service Candidate Development Program* and the *Cornerstone Program*. Numerous staff also spoke at conferences sponsored by prominent national associations for privacy and disclosure professionals.

DHS Leadership Year: The Privacy Office enthusiastically supported multiple workshops and training events as part of the DHS Leadership Year, a Department-wide effort to focus on the importance—and qualities that are demanded of—leaders in the public sector. The CPO sponsored several events, including a recognition ceremony for disclosure professionals with the DHS Deputy Secretary, a career-shadowing event with college students, and a panel discussion with former Chief Privacy Officers that was attended by representatives from more than a dozen DHS Components.

Student Mentoring: The Privacy Office partnered with colleges and universities across the nation to provide opportunities for four student internships within the Privacy Office. These law and undergraduate student interns supported projects with every team in the Privacy Office, making an essential contribution to our mission while gaining valuable career insight and experience.

V. Component Privacy Programs

DHS has a strong, dedicated network of Component privacy officers and PPOCs who work with the Privacy Office to ensure that Department activities incorporate privacy protections from the earliest stages of system and program development. In fact, every Component is required by DHS policy⁴⁰ to appoint a Privacy Officer to oversee privacy compliance, policy, and oversight activities in coordination with the CPO.

These privacy officers are the “boots on the ground” who are most familiar with DHS programs and systems, and can identify where the potential privacy issues may arise. They provide operational insight, support, and privacy expertise for Component activities. This section highlights the activities of Component privacy offices during this reporting period.

In addition, Component privacy offices conduct privacy training and host periodic events to raise privacy awareness and promote a culture of privacy. All Component training and awareness activities are described in our semi-annual [Section 803 Reports to Congress](#).

⁴⁰ See [DHS Privacy Policy Instruction 047-01-005, Component Privacy Officer](#).

Federal Emergency Management Agency (FEMA)



FEMA coordinates the Federal Government’s role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror. The FEMA Privacy Branch is located within the Information Management Division (IMD), which also includes the Records Management and Disclosure Branches. FEMA Privacy sustains privacy protections and minimizes privacy impacts on FEMA stakeholders.

FEMA Privacy engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Successfully closed out the recommendations from the June 2016 OIG Management Advisory Report, “FEMA Continues to Experience Challenges in Protecting Personally Identifiable Information at Disaster Recovery Centers.” FEMA hired the PPOC for the Disaster Operations program to expand FEMA Privacy’s footprint during disaster operations. This program ensures that at least one PPOC is designated to every disaster worksite to provide privacy training, disseminate privacy resource materials, and conduct privacy compliance site assessments.
- Continued to represent privacy interests on FEMA’s Strategic Leadership Steering Committee and Integrated Project Team (IPT) for FEMA’s agency-wide Workplace Transformation (WPT) Initiative.
- Conducted targeted PTA and PIA training to PPOCs, Information System Security Officers (ISSO), and other stakeholders within the National Capital Region (NCR), as well as FEMA Regional Offices.

-
- Represented privacy interests on several Agency-wide initiatives to consolidate and modernize legacy IT systems, including the Grants Modernization IPT and National Flood Insurance Program (NFIP) modernization efforts.
 - Represented privacy interests on the Information Governance Working Group (IGWG) as it relates to privacy topics surrounding the use of FEMA SharePoint collaboration sites, to ensure that proper privacy notifications are in place to inform employees how to appropriately protect PII on SharePoint.
 - Represented privacy and data protection interests as a permanent voting member of the FEMA Acquisition Review Board, where decisions are made regarding FEMA procurements involving PII.
 - Continued to serve as a permanent voting member of the FEMA Policy Working Group to ensure that all policies are developed in a way that minimizes privacy impacts.
 - Represented privacy and data protection interests as a member of the FEMA Data Governance Council, where decisions are made regarding the use of the agency's data assets involving PII. Collaborated with FEMA Data Governance Council's Data Management Team to conduct privacy training for FEMA data stewards and stakeholders.
 - Represented privacy and data protection interests as a member of the FEMA IT Governance Board, where decisions are made regarding the use of agency IT assets involving PII.

Privacy Compliance

FISMA scores: 98 percent for PIAs and 100 percent for SORNs.

All FEMA PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

Highlights of privacy compliance documents published during this report period:

Privacy Impact Assessments:

- [DHS/FEMA/PIA-049 Individual Assistance Program PIA](#): The Office of Response and Recovery (ORR) Individual Assistance (IA) Division completed this PIA. The IA Division manages the Individual Assistance programs that provide disaster recovery assistance to individuals and supports FEMA's recovery mission. The provision of the Individual Assistance programs require the collection and use of PII and Sensitive PII from applicants, which is accomplished through IT systems, applications, and forms. FEMA published this PIA to discuss individual assistance from a programmatic standpoint, to include the initial collection of information, its use and storage, and the associated technologies and tools used to support the program. FEMA streamlined the compliance process to allow for broader compliance coverage for IT systems, applications, and forms used to support the Individual Assistance program.
- [DHS/FEMA/PIA-050 National Flood Insurance Program PIVOT PIA](#): FEMA developed the PIVOT (not an acronym) system as part of an IT system modernization effort. PIVOT is a web-based IT solution for NFIP to replace the legacy IT systems and to help consolidate and facilitate the NFIP's core business processes. NFIP PIVOT allows FEMA to improve oversight of NFIP by modernizing NFIP's legacy NFIP IT system and consolidating other NFIP standalone systems.

National Protection and Programs Directorate (NPPD)



NPPD leads the national effort to protect and enhance the resilience of the nation’s physical and cyber infrastructure. The NPPD Office of Privacy supports a number of significant activities to promote and protect privacy while supporting critical mission operations at NPPD, including the Federal Protective Service (FPS), OBIM, Office of Infrastructure Protection (IP), Office of Cyber and Infrastructure Analysis (OCIA), and Office of Cybersecurity and Communications (CS&C).

Privacy Policy and Compliance Leadership

- Conducted, in collaboration with the Department of Justice’s Office of Privacy and Civil Liberties, the statutorily-required biennial review of the [Cybersecurity Information Sharing Act of 2015 \(CISA\) Privacy and Civil Liberties Final Guidelines](#).
- Conducted two Privacy Oversight Reviews⁴¹ of NPPD’s cybersecurity programs, specifically focused on CS&C’s EINSTEIN intrusion detection system, the Cyber Information Sharing and Collaboration Program (CISCP), and the AIS initiative. During these reviews, the NPPD Office of Privacy examined EINSTEIN 2 signatures, CISCP indicator bulletins, and AIS privacy rules to ensure that PII is not collected unnecessarily, and is handled appropriately as these programs effectively execute NPPD’s cybersecurity mission.
- Conducted a self-audit of NPPD contributions to the Nationwide Suspicious Activity Reporting Initiative in response to a letter from the DHS CPO. NPPD Office of Privacy and

⁴¹ In response to a 2011 Privacy Compliance Review recommendation by the DHS Privacy Office on NPPD’s handling of cybersecurity-related PII, the NPPD Office of Privacy instituted a regularly occurring “Privacy Oversight Review” process. The primary objective of these reviews is to assess NPPD’s cybersecurity programs and their operational products and activities, and to provide recommendations to ensure that privacy controls and safeguards continue to operate effectively and efficiently in all aspects where PII may be collected, used, or shared.

the FPS completed a self-audit of its 2017 contributions to eGuardian to ensure its contributions warranted continued retention, removing contributions in some cases.

- Played a critical role in an information security-based ongoing authorization working group, connecting with privacy offices across the interagency in an effort to establish a holistic current-state picture of agency privacy continuous monitoring strategies.
- Participated in the Privacy Office assessments of NPPD activities under Executive Order 13636 and Executive Order 13691.
- Conducted 400 privacy subject matter expert reviews as part of the IT Acquisition Review (ITAR) process to ensure core privacy clauses are included whenever contracted services may involve access to PII.

The NPPD Office of Privacy also contributed to the federal privacy enterprise through the following activities:

- NPPD's Privacy Officer continued collaborating with NIST's Privacy Engineering Program by providing outreach and education on the privacy requirements and considerations included in the NIST Special Publication (SP) 800-63, Digital Identity Guidelines (June 22, 2017). This included presentations at the Federal Privacy Council Privacy Summit, on an IAPP webinar, and at the 2018 RSA Conference in San Francisco, CA.
- NPPD Office of Privacy continued its contributions to the Federal Privacy Council by developing content for and teaching sessions of the "Privacy Boot Camp" on IT security for privacy professionals, as well as on web privacy policies and best practices to ensure the privacy of mobile applications.
- OBIM's Privacy, Policy, and FOIA Section Chief spoke about the FIPPs and privacy protections in the Automated Biometric Identification System (IDENT) at the Federal Identity Forum's Screening and Interoperability panel in September 2017, the Federal Privacy Council (FPC) Privacy Summit's Biometrics panel in December 2017, and the Biometric Institute's U.S. Conference Relationship of Trust panel in March 2018.
- The NPPD Office of Privacy also actively engaged with CS&C's Federal Network Resilience (FNR) division on its current state analysis of ongoing authorization efforts within the federal civilian enterprise. In order to conduct this analysis, FNR examined information security continuous monitoring and privacy continuous monitoring strategies throughout the interagency. The NPPD Office of Privacy connected FNR with appropriate interagency PPOCs and organized several meetings to discuss how privacy continuous monitoring effects agency ongoing authorization efforts. This input was gathered by FNR, and will be included in a forthcoming report.
- The NPPD Office of Privacy staff are actively engaged with the Federal Privacy Council by attending or participating in its training events and working groups. CS&C's senior privacy analyst is currently serving as co-chair on the Digital Privacy Subcommittee under the Federal Privacy Council's Technology and Innovation Committee. CS&C's other dedicated privacy analyst also serves as a member of this Subcommittee.

Privacy Compliance

FISMA scores: 100 percent for both PIAs and SORNs.

All NPPD PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the DHS Privacy Office website: www.dhs.gov/privacy.

Highlights of privacy compliance documents published during the reporting period:

Privacy Impact Assessments:

- [DHS/NPPD/PIA-010 FPS Dispatch Incident Records Management System](#): FPS owns and operates a suite of systems used to support nationwide incident reporting. This suite of systems is referred to in the PIA as the FPS Dispatch and Incident Record Management Systems (DIRMS). These systems are used by federal employees and contractors to document and report suspicious activities, security-related matters, and alleged violations of law related to the protection of federal facilities.
- [DHS/NPPD/PIA-009 Chemical Facility Anti-Terrorism Standards \(CFATS\)](#): The PIA was updated to describe the potential privacy risks resulting from the Department's implementation of an enhanced methodology for using risk-based tiers under the CFATS program.
- [DHS/NPPD/PIA-020 Private Sector Clearance Program for Critical Infrastructure](#): The PIA was updated to clarify the role that PSCP plays in the clearance process for private sector partners across NPPD, and to describe the collection of additional data elements through DHS Form 9014 from applicants who require clearances based on their work in relation to security of critical infrastructure.
- [DHS/NPPD/PIA-002 Automated Biometric Identification System \(IDENT\)](#): OBIM Privacy drafted PIA updates to address increased sharing and cooperation with New Zealand and Mexico:
 - The New Zealand IDENT PIA Sub-Appendix allows New Zealand to search the IDENT database for automated information sharing in order to administer or enforce immigration laws, determine visa eligibility and immigration benefits, and increase collaboration on border security, and identity fraud.
 - The Mexico PIA Sub-Appendix allows for Mexico to search IDENT for biometric and associated biographic data on Third Country Nationals collected by Mexico's National Institute of Migration, in coordination with the Department of State.

Office of Intelligence and Analysis (I&A)

I&A is responsible for collecting, analyzing, producing, and disseminating intelligence and information needed to keep the homeland safe, secure, and resilient. I&A provides intelligence support across the full range of DHS mission areas to DHS and its Components; state, local, tribal, and territorial governments; and the private sector. I&A's Privacy Officer ensures that I&A intelligence activities are conducted in a manner that appropriately protects individuals' privacy through a variety of activities that are highlighted below. In addition, the I&A Privacy Officer serves as the Intelligence Oversight Officer, with responsibilities to ensure compliance with [Executive Order 12333](#), *U.S. Intelligence Activities*, and other intelligence-related authorities. These responsibilities intersect with privacy compliance because intelligence authorities include specific requirements for handling the PII of U.S. Persons.

I&A Privacy engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Participated as a key member in numerous agency-wide groups and committees, including the DARC and the Data Framework Working Group.

Privacy Compliance

- I&A, as an element of the IC, is exempt from FISMA reporting requirements.
- Collaborates with program offices to produce privacy compliance documentation for privacy-sensitive systems and programs. While the vast majority of these documents are not made public, they do serve important roles in technology development, decision-making, and in raising staff awareness concerning privacy matters at I&A.
- Partners with the CIO to ensure that privacy documentation is in place before any new IT investment is approved.
- Partners with I&A's Office of Procurement to ensure that the proper Privacy Act compliance language is present in all appropriate contracts.

Transportation Security Administration (TSA)



TSA is responsible for protecting the Nation's transportation systems to ensure freedom of movement for people and commerce. TSA is most visible through its aviation security efforts, but is also responsible for the security of other modes of transportation, including highways and motor carriers, mass transit, freight rail, oil, and natural gas pipelines, and in coordination with the United States Coast Guard (USCG), maritime.

The TSA Privacy Office (TSA Privacy) engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Provided continuous advice and oversight on:
 - passenger screening protocols;
 - security technology initiatives, including Advanced Imaging Technology improvements and Stand-Off Detection;
 - information sharing requests and initiatives;
 - the use of biometrics at airport checkpoints;
 - expanding derogatory data sets in vetting of transportation sector workers;
 - the development of the TSA Insider Threat Program;
 - use of social media for vetting of transportation sector workers; and
 - TSA watch lists.
- As a member of the TSA Security Threat Assessment Board, TSA Privacy provided a privacy and civil liberties review of proposed actions to revoke transportation sector worker credentials. TSA Privacy also provided 24/7 reviews of law enforcement agency requests for Secure Flight passenger information under the Privacy Act.

Privacy Compliance

- FISMA scores: 100 percent for both PIAs and SORNs.
- Conducted annual reviews of 11 programs to ensure that PIAs adequately represented the program.
- Reviewed more than 400 pending contract actions to implement PII handling and breach remediation requirements as necessary, and to ensure that any other privacy compliance requirements implicated by the contract were completed.

All TSA PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the DHS Privacy Office website: www.dhs.gov/privacy.

United States Citizenship and Immigration Services (USCIS)



The USCIS Office of Privacy works diligently to promote a culture of privacy throughout all USCIS operations by: training staff, identifying best practices, developing policies, reviewing contracts and proposed and existing uses of technology for compliance with federal law and the FIPPs, participating in USCIS working groups, integrating privacy controls into the IT system development life cycle, and conducting operational site assessments to identify agency risks.

USCIS Privacy engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Provided guidance to USCIS's programs and directorates to ensure the implementation of operational use of social media to protect the privacy, civil rights, and civil liberties of those who will be subject to social media searches.
- Provided privacy risk-based analysis on DHS and government-wide operations, legislative proposals, and Executive Orders.
- Developed and delivered a variety of privacy-related training to USCIS personnel and key stakeholders, including a refresher training on how to identify and protect Section 1367 information within files and electronic systems.
- Developed and implemented a process to ensure that all unauthorized disclosures of Section 1367 information are reported through the privacy incident reporting process and CRCL.
- Broadcast a video featuring the USCIS Privacy Officer to promote privacy awareness throughout the agency.
- Facilitated information sharing requirements between internal and external stakeholders (federal, state, local, and international organizations) to ensure that such sharing is conducted in compliance with applicable privacy law and policy.

-
- Integrated privacy by design principles into the IT system development life cycle using a risk-based approach in accordance with NIST guidelines.
 - Monitored and reviewed multiple IT development projects to ensure that privacy requirements are considered throughout the Agile lifecycle.
 - Conducted 50 site visits to USCIS facilities throughout the country to promote privacy protection best practices related to immigration operations.
 - Provided guidance to Contract Officers (CO), Contract Officer's Representatives (COR), and Program Managers on the process for completing the Homeland Security Acquisition Manual Appendix G Form for identifying high-risk contracts.
 - Met with major U.S. courier companies on the appropriate handling of USCIS shipments containing sensitive records to prevent the loss and/or mishandling of USCIS shipments, and to ensure compliance with the awarded contract.

Privacy Compliance

- FISMA scores: 90 percent for PIAs and 97 percent for SORNs.
- Participated in working groups to implement Section 14 of *Executive Order 13768, Enhancing Public Safety in the Interior of the United States*.
- Reviewed over 280 contracts to add privacy clauses, as needed, to protect and secure PII that is shared with USCIS partners.
- Conducted seven privacy security compliance reviews within USCIS HQ, to identify potential privacy and security vulnerabilities, and to assess compliance with USCIS and DHS security and privacy policies on securing and safeguarding Sensitive PII and classified information.

All USCIS PIAs and SORNs published during the reporting period are listed in Appendix D and can be found on the DHS Privacy Office website: www.dhs.gov/privacy.

Highlights of privacy compliance documents published during the reporting period:

- [DHS/USCIS/PIA-071 myUSCIS Account Experience](#): USCIS operates myUSCIS Account Experience to engage benefit requestors and legal representatives while they navigate and complete the immigration process through an authenticated digital account experience. MyUSCIS Account Experience offers a personalized, authenticated, and secured account for benefit requestors and legal representatives, and replaces all aspects of the public facing USCIS Electronic Immigration System.
- [DHS/USCIS/ICE/CBP-001 – Alien File, Index, and National File Tracking System of Records](#): This system of records contains information regarding transactions involving an individual as he or she passes through the U.S. immigration process, some of which may also be covered by separate Systems of Records Notices. DHS primarily maintains information relating to the adjudication of benefits, investigation of immigration violations, and enforcement actions in Alien Files (A-Files).

United States Coast Guard (USCG)



USCG is the world's premier, multi-mission maritime service, responsible for the safety, security, and stewardship of the Nation's waters. The USCG employs its broad authorities; expansive network of interagency, military, and industry relationships; unique operational capabilities; and international partnerships to execute daily, steady-state operations, and respond to major incidents.

The USCG Privacy Office engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Collaborated with the USCG Operations Center and posted a warning banner restricting Sensitive PII on the USCG FIX IT help desk site.
- Provided biweekly training to over 270 new USCG civilian employees emphasizing the importance of safeguarding PII.
- Created and disseminated a weekly overview of current and emergent USCG privacy activities to senior leadership.
- Served as a member of the USCG Operational Social Media Integrated Project Team (IPT) that is researching several social media platforms to facilitate various agency operational functions and activities.
- Attended monthly meetings with the USCG Health Insurance Portability and Accountability Act (HIPAA) representative to ensure privacy oversight, and to mitigate privacy incidents involving personal health information.
- Collaborated with the USCG Office of Information Assurance to provide privacy incident metrics for the evaluation of DHS's information security program audit.

Privacy Compliance

- FISMA scores: 100 percent for both PIAs and SORNs.
- Reviewed USCG directives, forms, and information collection as a part of the clearance process, resulting in the submission of compliance documentation to ensure adherence to current federal privacy mandates.
- Developed initial privacy compliance documentation to utilize social media during Hurricanes Harvey and Maria for situational awareness and search and rescue operations.
- Reviewed over 200 IT Acquisition Reviews (ITAR), confirming requisite privacy documentation and ensuring core clauses were included in contracted services involving access to PII.

All USCG PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the DHS Privacy Office website: www.dhs.gov/privacy.

U.S. Customs and Border Protection (CBP)



CBP is one of the world's largest law enforcement organizations, charged with securing our borders while facilitating lawful international travel and trade. As the United States' first unified border entity, CBP takes a comprehensive approach to border management and control, combining customs, immigration, border security, and agricultural protection into one coordinated and supportive activity.

The CBP Privacy Office (CBP Privacy) engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Hired two new Branch Chiefs to support the CBP Privacy Officer in the management of privacy compliance, policy, and oversight functions. The Branch Chiefs provide privacy guidance and expertise to CBP offices.
- Developed and implemented new Standard Operating Procedures (SOP) for the office's management of Privacy Incidents and Information Breaches, as well as the conduct of CBP Privacy Evaluations, comprised of programmatic reviews designed to identify and address privacy compliance gaps and risks.
- Formed a staff-led working group to review and update the Agency's Directive on the Operational Use of Social Media to ensure that CBP's use of social media tools is consistent with both legal requirements and DHS policy.
- Initiated a systematic review of CBP's information request and disclosure processes in order to identify, develop, and implement more efficient practices, allowing CBP to share law enforcement information in a more complete and timely manner.
- Collaborated with CBP's Office of Public Affairs, Office of Field Operations, U.S. Border Patrol, Office of the Chief Counsel, and Office of Policy to review proposed releases of information to the media about non-U.S. citizen/non-Lawful Permanent Residents.

Privacy Compliance

- FISMA scores: 98 percent for PIAs and 100 percent for SORNs.
- Continued to expand the privacy compliance program by requiring PTAs for all forms and information collections, ongoing information sharing initiatives, and all individual sub-systems to improve visibility into what information is being collected, maintained, and shared, and to ensure sufficient PIA and SORN coverage for all IT systems.
- Developed the CBP Privacy Evaluation (CPE), an internal review similar to the DHS PCR process, to facilitate assessment of programs and systems for compliance with policies, procedures and best practices for managing PII in accordance with the FIPPs.
- Worked with the Privacy Office to complete a PCR for the Electronic System for Travel Authorization (ESTA), focusing on the program's use of social media identifiers in the screening and vetting of ESTA applicants from Visa Waiver Program countries. The PCR found that the program was sufficiently compliant with established privacy-protective practices and principles. However, the Privacy Office recommended that CBP develop a more robust means of tracking the efficacy of the use of social media identifiers in the screening and vetting process.

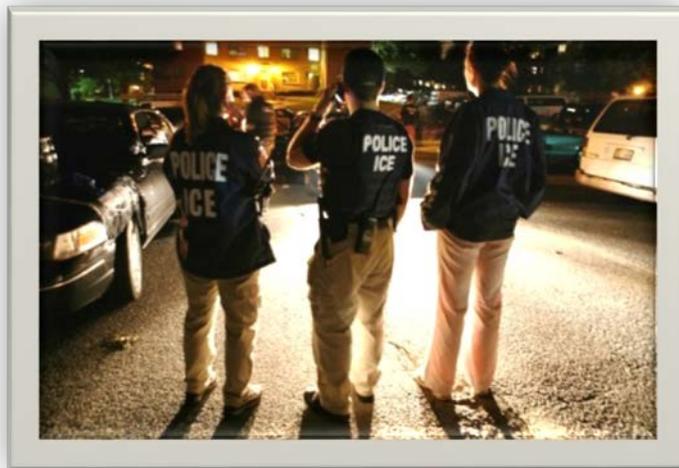
All CBP PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the DHS Privacy Office website: www.dhs.gov/privacy.

Highlights of privacy compliance documents published during the reporting period:

Privacy Impact Assessments:

- [DHS/CBP/PIA-008 – Border Searches of Electronic Devices](#): CBP published this PIA update to describe changes to, and the reissuance of, CBP's policy directive governing border searches of electronic devices, CBP Directive No. 3340-049A, Border Searches of Electronic Devices (January 2018). The updated PIA assesses the new risks associated with the prevalence of smart phones and cloud computing, and discusses how the new Directive assists in mitigating these risks.
- [DHS/CBP/PIA-051 Automated Passport Control \(APC\) and Mobile Passport Control \(MPC\)](#): CBP developed the APC and MPC programs to automate and expedite eligible travelers' entry process into the United States. These programs enable travelers to perform select entry declaration and inspection requirements tasks through a self-service kiosk (APC) or a mobile device application (MPC). CBP published a PIA to explain how these programs facilitate the inspection process while enabling the secure transmission of information from members of the public to CBP.
- [DHS/CBP/PIA-052 Incident-Driven Video Recording Systems \(IDVRS\) Evaluation](#): In 2018, CBP began conducting a field evaluation of IDVRS throughout its law enforcement operations to determine the effectiveness of fixed, vehicle, and body-worn camera technology to provide an accurate representation of law enforcement encounters, while allowing CBP Officers/Agents to safely perform their duties. CBP published a PIA to provide notice to the public of this new use of technology, and to evaluate the privacy risks associated with CBP's use of incident-driven video recording technology at and between U.S. ports of entry.

U. S. Immigration and Customs Enforcement (ICE)



ICE's mission is to protect America from cross-border crime and illegal immigration that threaten national security and public safety. This mission is executed through the enforcement of more than 400 federal statutes and focuses on effective immigration enforcement, preventing terrorism and combating the illegal movement of people and goods.

The ICE Privacy Office (ICE Privacy) engaged in the following significant activities during the reporting period:

Privacy Policy Leadership

- Continued to process Privacy Act access and amendment requests received from the FBI Criminal Justice Information Services (CJIS). ICE works with CJIS to ensure that information from ICE, legacy Immigration and Naturalization Service, or legacy U.S. Customs Service arrests maintained in FBI records is accurate and complete.
- Provided internal agency guidance on access to and use of License Plate Reader (LPR) data and technology.
- Established a process to assist the ICE Office of Congressional Relations in disclosing information about ICE Enforcement and Removal Operations (ERO) high profile removals to Congress.

Privacy Compliance

- FISMA scores: 93 percent for PIAs and 100 percent for SORNs.
- Completed or updated 45 PTAs, three PIAs, two SORNs, one Notice of Proposed Rulemaking, nine Disposition PTAs, and nine Testing Questionnaires during the reporting period.
- Responded to six Privacy Act amendment requests, and received no privacy complaints.
- Reviewed over 175 proposed procurements to ensure the inclusion of appropriate privacy protections in contract language.

-
- Resolved an estimated 75 privacy incidents, taking various steps to mitigate any damages from the incidents and prevent future incidents.
 - Provided advice and oversight during the development of 16 Information Sharing Agreements signed during the reporting period.

All ICE PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the DHS Privacy Office website: www.dhs.gov/privacy.

Highlights of privacy compliance documents published during the reporting period:

Privacy Impact Assessments:

- [DHS-ICE-PIA-039 Acquisition and Use of License Plate Reader Data from a Commercial Service](#): This PIA Update explains ICE’s operational use of the service, and describes the privacy and civil liberties protections implemented by the agency and the vendor. ICE procured query-based access to a vendor-owned commercial License Plate Reader (LPR) data service that stores recorded vehicle license plate data from cameras equipped with license plate reader technology. ICE uses LPR data from this service in support of its criminal and administrative law enforcement missions. In March 2015, ICE published a PIA announcing ICE’s intention to procure access to a commercial LPR database and describing the controls ICE would put in place to ensure the agency complies with privacy and civil liberties requirements when using the service.
- [DHS/ICE/PIA-048 Data Analysis System \(DAS\)](#): DAS is an analytical database owned, operated, and maintained by ERO. The National Criminal Analysis and Targeting Center (NCATC), located within ERO’s Targeting Operations Division, uses DAS to assist ERO field offices in locating aliens convicted of criminal offenses and other aliens who are amenable to removal. DAS was first deployed in 2006, and a discussion of the system was included in the PIA for the Fugitive Case Management System (FMCS), which has been dispositioned.
- [DHS/ICE/PIA-037\(a\) electronic Health Records \(eHR\) System](#): eHR is an ICE case management system for maintaining records of medical treatment provided to individuals detained by ICE. ICE detainees receive medical, dental, and mental health evaluations. This PIA Update describes ICE’s development of an online Patient Medical Record Portal in which former detainees can access an electronic copy of their medical records.

System of Records Notices:

- [DHS/ICE-013 Alien Health Records System](#): This SORN modifies and reissues a current ICE system of records titled, “*DHS/ICE–013 Alien Health Records System.*” This updated system of records allows the Department to maintain records that document the health screening, examination, and treatment of aliens arrested by the Department and detained by ICE for civil immigration purposes in facilities where the ICE Health Service Corps (IHSC) provides or oversees the provision of care. This SORN Update describes IHSC’s

development of a Patient Medical Record Portal, whereby former ICE detainees can access an electronic copy of their medical records.

- [DHS/ICE-007 Criminal History and Immigration Verification \(CHIVe\) System of Records:](#)
This SORN modifies, renames, and reissues a current “*DHS/ICE–007 Alien Criminal Response Information Management (ACRIMe)*.” This system of records allows ICE to receive and respond to criminal history and immigration status inquiries made by federal, state, and local law enforcement agencies, and other federal agencies, including the Office of Personnel Management (OPM) and the Department of Health and Human Services (HHS). This SORN Update allows ICE to share immigration-related information and criminal history summary information with HHS relating to potential sponsors of unaccompanied alien children and other adult members of the potential sponsors’ households.

United States Secret Service (USSS or Secret Service)



The Secret Service safeguards the Nation's financial infrastructure and payment systems to preserve the integrity of the economy, and protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events.

The USSS FOIA & Privacy Act Program (USSS Privacy) engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- In response to the 2017 Privacy Office's PCR of the USSS Privacy Office, USSS senior leadership along with USSS Privacy Office management took significant steps to implement the PCR recommendations to strengthen USSS Privacy Office operations and to promote a culture of privacy within the agency.
- Created and filled a dedicated Privacy Officer position.
- Continued to participate in the USSS PII Working Group to assess the use, collection, maintenance, and safeguarding of PII.
- Represented privacy and data protection interests as a member of the Enterprise Governance Council, where decisions are made about USSS's funding, procurement, and use of IT assets that involve the collection, use, maintenance, and dissemination of PII.
- Promoted privacy awareness with posters and electronic kiosks throughout the USSS Headquarters building.
- Provided advice to USSS personnel on the collection, maintenance, use, handling, dissemination, and safeguarding of USSS data to ensure compliance with the FIPPs.

Privacy Compliance

- FISMA scores: 100 percent for PIAs and SORNs.
- Reviewed and drafted Privacy Act statements for new and existing USSS forms.
- Reviewed IT waiver and/or exception requests submitted by the OCIO for systems processing PII to assess privacy implications.
- Collaborated with the USSS Inspection Division to include privacy compliance equities on its official Checklist when it conducts quadrennial compliance inspections of all USSS offices to reinforce the need to protect PII.

All USSS PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the DHS Privacy Office website: www.dhs.gov/privacy.

Appendix A – Acronyms

Acronyms	
AFI	Analytical Framework for Intelligence
AIS	Automated Indicator Sharing
ATO	Authority to Operate
ATS	Automated Targeting System
CBP	U.S. Customs and Border Protection
CFO	Chief Financial Officer
CHCO	Chief Human Capital Office or Officer
CIO	Chief Information Officer
CISA	Cybersecurity and Information Sharing Act of 2015
CMA	Computer Matching Agreement
CPO	Chief Privacy Officer
COR	Contracting Officer Representative
CRCL	Office for Civil Rights and Civil Liberties
CS&C	Office of Cybersecurity & Communications in NPPD
CUI	Controlled Unclassified Information
CVE	Countering Violent Extremism
CVTF	Common Vetting Task Force
DARC	Data Access Review Council
DHS	Department of Homeland Security
DHS TRIP	DHS Traveler Redress Inquiry Program
DMAG	Deputy Secretary’s Management Action Group
DOJ	Department of Justice
DPIAC	Data Privacy and Integrity Advisory Committee
E3A	EINSTEIN 3 Accelerated Program
ECS	Enhanced Cybersecurity Services
EO	Executive Order
ESTA	Electronic System for Travel Authorization
EU	European Union
FACA	Federal Advisory Committee Act
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCC	Five Country Conference
FEMA	Federal Emergency Management Agency
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Centers
FOIA	Freedom of Information Act
FPS	Federal Protective Service

Acronyms	
FY	Fiscal Year
GSA	General Services Administration
HR	Human Resources
HSIN	Homeland Security Information Network
HQ	Headquarters
HSI	Homeland Security Investigations
I&A	Office of Intelligence and Analysis
IAPP	International Association of Privacy Professionals
IC	Intelligence Community
ICAM	Identity, Credentialing, and Access Management
ICE	United States Immigration and Customs Enforcement
IIR	Intelligence Information Report
ISAA	Information Sharing Access Agreement
ISAO	Information Sharing Analysis Organization
ISSGB	Information Sharing and Safeguarding Governance Board
ISSM	Information Security System Manager
ISSO	Information Security System Officer
IT	Information Technology
ITAR	Information Technology Acquisition Review
ITP	Insider Threat Program
JRC	Joint Requirements Council
MMC	Media Monitoring Capability
NARA	National Archives and Records Administration
NCCIC	National Cybersecurity and Communications Integration Center
NCR	National Capital Region
NCTC	National Counterterrorism Center
NFIP	National Flood Insurance Program
NIST	National Institute for Standards and Technology
NOC	National Operations Center
NPPD	National Protection and Programs Directorate
NPRM	Notice of Proposed Rulemaking
OBIM	Office of Biometric Identity Management
OCSO	Office of the Chief Security Officer
ODNI	Office of the Director of National Intelligence
OGC	Office of the General Counsel
OGIS	Office of Government Information Services
OIA	TSA's Office of Intelligence and Analysis
OIG	Office of Inspector General
OIP	DOJ Office of Information Policy
OMB	Office of Management and Budget
OPS	Office of Operations Coordination

Acronyms	
OPM	Office of Personnel Management
PACT	Privacy Administrative Coordination Team
P/CL	Privacy and civil liberties
PCLOB	Privacy and Civil Liberties Oversight Board
PCR	Privacy Compliance Review
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIHG	DHS Privacy Incident Handling Guidance
PIV	Personal Identity Verification
PLCY	Office of Policy
PNR	Passenger Name Records
PPD	Presidential Policy Directive
PPOC	Privacy Point of Contact
PRA	Paperwork Reduction Act
PTA	Privacy Threshold Analysis
RFI	Request for Information
RO	Reports Officer
S&T	Science and Technology Directorate
SAC	Staff Advisory Council
SAOP	Senior Agency Officials for Privacy
SBA	United States Small Business Administration
SBU	Sensitive but Unclassified
SCO	Screening Coordination Office
SLTT	State, Local and Tribal Territories
SME	Subject Matter Expert
SMOUT	Social Media Operational Use Template
SOC	Security Operations Center
SORN	System of Records Notice
SOP	Standard operating procedure
SOW	Statement of Work
SSI	Sensitive Security Information
TSA	Transportation Security Administration
UAS	Unmanned Aircraft Systems
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service

Appendix B – DHS Implementation of the Fair Information Practice Principles (FIPPs)

DHS's implementation of the FIPPs is described below:

Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

Individual Participation: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Purpose Specification: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration.

Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Data Quality and Integrity: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Security: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Appendix C – Compliance Activities

The Privacy Compliance Process

DHS systems, initiatives, and programs must undergo the privacy compliance process, which consists of completing privacy compliance documentation and undergoing periodic reviews of existing programs to ensure continued compliance.

The Privacy Office, in collaboration with the CIO, Chief Information Security Officer, and Chief Financial Officer (CFO), identifies programs that must be reviewed for privacy compliance through several avenues including:

- (1) the FISMA Security Authorization process, which identifies IT systems that must meet privacy requirements under FISMA;
- (2) the OMB IT budget submission process, which requires the Privacy Office to review all major DHS IT investments and associated systems on an annual basis, prior to submission to OMB for inclusion in the President’s annual budget, to ensure that proper privacy protections and privacy documentation are in place;⁴²
- (3) CIO IT Program Reviews, which are comprehensive reviews of existing major IT investments and include a check for accurate and up-to-date privacy compliance documentation; and,
- (4) PRA processes, which require the Privacy Office to review DHS forms that collect PII to ensure that only the information needed to fulfil the purpose of the collection is required on forms. This review also ensures compliance with the Privacy Act Statement requirement, pursuant to 5 U.S.C. § 552a(e)(3).

Privacy Compliance Documents: Keys to Transparency and Accountability

The DHS privacy compliance documentation process includes three primary documents: (1) the PTA, (2) the PIA, and (3) the SORN. Each of these documents has a distinct function in implementing privacy policy at DHS, but together they further the transparency of Department activities and demonstrate accountability.

PTAs

The first step in the process is for DHS staff seeking to implement or modify a system, program, technology, or rulemaking to complete a PTA. The Privacy Office reviews and adjudicates the PTA. This document serves as the official determination as to whether or not the system, program, technology, or rulemaking is privacy sensitive (i.e., involves the collection and use of PII) and requires additional privacy compliance documentation such as a PIA or SORN.

⁴² See Office of Management & Budget, Executive Office of the President, OMB Circular No. A-11, Section 31.8, *Management improvement initiatives and policies*, available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/assets/a11_current_year/a11_2017.pdf.

PIAs

The E-Government Act of 2002 and the Homeland Security Act require PIAs. PIAs may also be required in accordance with DHS policy issued pursuant to the CPO's statutory authority. PIAs are an important tool for examining the privacy impact of IT systems, initiatives, programs, technologies, or rulemakings. The PIA is based on the FIPPs framework and covers areas such as the scope and use of information collected, information security, and information sharing. Each section of the PIA concludes with analysis designed to outline any potential privacy risks identified in the answers to the preceding questions and to discuss any strategies or practices used to mitigate those risks. The analysis section reinforces critical thinking about ways to enhance the natural course of system development by including privacy in the early stages.

If a PIA is required, the relevant personnel will draft the PIA for review by the Component privacy officer or PPOC and Component counsel. Part of the PIA analysis includes determining whether an existing SORN appropriately covers the activity or a new SORN is required. Once the PIA is approved at the Component level, the Component privacy officer or PPOC submits it to the Privacy Office Compliance Team for review and approval. The CPO signs the final PIA when satisfied with the privacy risk mitigations. Once approved, PIAs are published on the Privacy Office website, with the exception of a small number of PIAs that are Law Enforcement Sensitive or classified for national security reasons.

PIAs are required when developing or issuing any of the following:

- **IT systems** that involve PII of members of the public, as required by Section 208 of the E-Government Act;
- **Proposed rulemakings** that affect PII, as required by Section 222 (4) of the Homeland Security Act [6 U.S.C. § 142(a)(4)];
- **Human resource IT systems** that affect multiple DHS Components, at the direction of the CPO;
- **National security systems** that affect PII, at the direction of the CPO;
- **Program PIAs**, when a program or activity raises privacy concerns;
- **Privacy-sensitive technology PIAs**, based on the size and nature of the population impacted, the nature of the technology, and whether the use of the technology is high profile; and,
- **Pilot testing** when testing involves the collection or use of PII.

SORNs

The Privacy Act requires that federal agencies issue a SORN to provide the public notice regarding personal information collected in a system of records.⁴³ SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security, or other reasons. If a SORN is required, the program manager will work with the Component privacy officer or PPOC and Component counsel to write the SORN for submission to the Privacy Office. As with the PIA, the CPO reviews, signs, and publishes all SORNs for the Department.

Periodic Reviews

Once the PTA, PIA, and SORN are completed, they are reviewed periodically by the Privacy Office (timing varies by document type and date approved). For systems that require only PTAs and PIAs, the process begins again three years after the document is complete or when there is an update to the program, whichever comes first. The process begins with either the update or submission of a new PTA. OMB guidance requires that SORNs be reviewed on a biennial basis.⁴⁴

⁴³ 5 U.S.C. § 552a(e)(4).

⁴⁴ Office of Management & Budget, Executive Office of the President, OMB Circular No. A-130, *Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals*, (November 28, 2000), available at http://www.whitehouse.gov/omb/circulars_a130_a130trans4. It should be noted that OMB Circular No. A-130 was revised on July 28, 2016, and can be found here: <https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>. The prior version of Appendix I of A-130 has become OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A108/omb_circular_a-108.pdf, which was released on December 23, 2016, at 81 FR 94424.

Appendix D – Published PIAs and SORNs

Privacy Impact Assessments Published July 1, 2017 – June 30, 2018		
Component	Name of System	Date Published
CBP	DHS/CBP/PIA-044 Joint Integrity Case Management System (JICMS)	07/18/2017
CBP	DHS/CBP/PIA-012(a) CBP Portal (e3) to ENFORCE/IDENT	08/10/2017
CBP	DHS/CBP/PIA-002(d) Global Enrollment System (GES): Trusted Traveler Program (TTP) System	08/15/2017
CBP	DHS/CBP/PIA-045 Assaults and Use of Force Reporting System (AUFRS)	08/24/2017
CBP	DHS/CBP/PIA-046 Border Patrol Enforcement Tracking System (BPETS/BPETS2)	08/28/2017
CBP	DHS/CBP/PIA-047 Firearms, Armor, and Credentials Tracking System (FACTS)	08/30/2017
CBP	DHS/CBP/PIA-016(a) I-94 Website Application	09/06/2017
CBP	DHS/CBP/PIA-030(d) Traveler Verification Service (TVS): CBP-TSA Technical Demonstration	09/25/2017
CBP	DHS/CBP/PIA-048 Academy Class Management System (ACMS.net)	12/08/2017
CBP	DHS/CBP/PIA-049 CBP License Plate Reader Technology	12/15/2017
CBP	DHS/CBP/PIA-050 United States - Mexico Entry/Exit Data Sharing Initiative	12/20/2017
CBP	DHS/CBP/PIA-008(a) Border Searches of Electronic Devices	01/05/2018
CBP	DHS/CBP/PIA-027(a) Southwest Border Pedestrian Exit Field Test	03/05/2018
CBP	DHS/CBP/PIA-051 Automated Passport Control (APC)/Mobile Passport Control (MPC)	03/19/2018
CBP	DHS/CBP/PIA-052 Incident-Driven Video Recording Systems (IDVRS) Evaluation	04/03/2018
CBP	DHS/CBP/PIA-018(a) Aircraft Systems	04/06/2018
CBP	DHS/CBP/PIA-053 U.S. Border Patrol Digital Forensics Programs	04/06/2018
CBP	DHS/CBP/PIA-054 Laboratory Information Network (LIN)	06/14/2018
CBP	DHS/CBP/PIA-014(a) Centralized Area Video Surveillance System	06/29/2018
DHS	DHS/ALL/PIA-039(a) Physical Access Control System (PACS)	07/21/2017

Privacy Impact Assessments Published July 1, 2017 – June 30, 2018		
Component	Name of System	Date Published
DHS	DHS/ALL/PIA/050 DHS Trusted Identity Exchange	07/24/2017
DHS	DHS/ALL/PIA-049(a) Performance and Learning Management System (PALMS)	08/31/2017
DHS	DHS/ALL/PIA-046(e) DHS Data Framework	10/10/2017
DHS	DHS/ALL/PIA-033 Use of Google Analytics	12/08/2017
DHS	DHS/OCHCO/PIA-063 Drug-Free Workplace Program	01/03/2018
DHS	DHS/ALL/PIA-052(a) DHS Insider Threat Program	03/02/2018
DHS	DHS/ALL/PIA-064 Greece and Italy Preventing and Combating Serious Crime Agreements	04/03/2018
DHS	DHS/ALL/PIA-002(b) Traveler Redress Inquiry Program	04/24/2018
DHS	DHS/ALL/PIA-065 Electronic Contract Filing System (ECFS)	06/07/2018
DHS	DHS/OCHCO/PIA-066 Employee Assistance Program	06/11/2018
FEMA	DHS/FEMA/PIA-040(a) Deployment Tracking System	07/20/2017
FEMA	DHS/FEMA/PIA-048 National Flood Insurance Program (NFIP) Direct Servicing Agent (NFIP Direct) System	10/31/2017
FEMA	DHS/FEMA/PIA-049 Individual Assistance (IA) Program	01/12/2018
FEMA	DHS/FEMA/PIA-050 National Flood Insurance Program (NFIP) PIVOT System	03/28/2018
FEMA	DHS/FEMA/PIA-009(a) Document Management and Records Tracking System (DMARTS)	04/06/2018
FEMA	DHS/FEMA/PIA-051 FEMA Physical Access Control Systems (PACS)	04/20/2018
FEMA	DHS/FEMA/PIA-020(b) Web-IFIMS (Integrated Financial Management Information System)	04/23/2018
FEMA	DHS/FEMA/PIA-018(a) FEMA Suspicious Activity Reporting (SAR)	06/06/2018
ICE	DHS/ICE/PIA-048 Data Analysis System (DAS)	09/29/2017
ICE	DHS/ICE/PIA-039(a) Acquisition and Use of License Plate Reader (LPR) Data from a Commercial Service	01/02/2018
ICE	DHS/ICE/PIA-037(a) electronic Health Records (eHR) System	05/01/2018

Privacy Impact Assessments Published July 1, 2017 – June 30, 2018		
Component	Name of System	Date Published
NPPD	DHS/NPPD/PIA-010(c) Federal Protective Service Dispatch and Incident Record Management Systems	07/18/2017
NPPD	DHS/NPPD/PIA-020(b) Private Sector Clearance Program for Critical Infrastructure (PSCP)	03/08/2018
TSA	DHS/TSA/PIA-046 Travel Document Checker Automation Using Facial Recognition	01/05/2018
TSA	DHS/TSA/PIA-047 TSA Contact Center	01/26/2018
USCG	DHS/USCG/PIA-025 Asset Logistics Management Information System (ALMIS)	01/30/2018
USCG	DHS/USCG/PIA-026 USCG Research and Development Center (RDC) small Unmanned Aircraft Systems (sUAS) Program	02/23/2018
USCG	DHS/USCG/PIA-023(a) Incident Reporting Information System	04/20/2018
USCG	DHS/USCG/PIA-027 Coast Guard Art Program Website	05/29/2018
USCIS	DHS/USCIS/PIA-027(c) Asylum Division	07/25/2017
USCIS	DHS/USCIS/PIA-068 Refugee Case Processing and Security Vetting	07/25/2017
USCIS	DHS/USCIS/PIA-018(a) Alien Change of Address Card (AR-11)	08/24/2017
USCIS	DHS/USCIS/PIA-017(a) Microfilm Digitization Application System (MiDAS)	08/31/2017
USCIS	DHS/USCIS/PIA-070 USCIS ServiceNow: Service Desk	08/31/2017
USCIS	DHS/USCIS/PIA-044 Validation Instrument for Business Enterprises (VIBE)	10/13/2017
USCIS	DHS/USCIS/PIA-046(a) Customer Scheduling and Services	12/08/2017
USCIS	DHS/USCIS/PIA-071 myUSCIS Account Experience	12/18/2017
USCIS	DHS/USCIS/PIA-060(a) Customer Profile Management System	02/07/2018
USCIS	DHS/USCIS/PIA-069 International Case Tracking System (ICTS)	02/07/2018
USCIS	DHS/USCIS/PIA-008(a) Enterprise Service Bus 2 (ESB 2)	03/12/2018
USCIS	DHS/USCIS/PIA-010 Person Centric Query Service	04/06/2018
USCIS	DHS/USCIS/PIA-012(a) Correspondence Handling and Management Planning System (CHAMPS)	04/12/2018

Privacy Impact Assessments Published July 1, 2017 – June 30, 2018		
Component	Name of System	Date Published
USCIS	DHS/USCIS/PIA-072 CAP Tracker	04/20/2018
USCIS	DHS/USCIS/PIA-038 FOIA/PA Information Processing System (FIPS)	06/01/2018
USSS	DHS/USSS/PIA-019 eCASE Management System	07/13/2017
USSS	DHS/USSS/PIA-020 United States Secret Service Counter Surveillance Division Unmanned Aerial Systems Program Test	08/02/2017
USSS	DHS/USSS/PIA-021 Comprehensive Incident Database on Targeted Violence (CID-TV)	05/07/2018
USSS	DHS/USSS/PIA-019 Radio Over IP (ROIP)	06/22/2018
USSS	DHS/USSS/PIA-016(a) Enterprise Person (ePerson) System	06/25/2018

System of Records Notices Published July 1, 2017 – June 30, 2018		
Component	Name of System	Date Published
DHS	DHS/ALL-038 Foreign Access Management System (FAMS)	07/27/2017
DHS	DHS/ALL-040 DHS Personnel Recovery Information	10/25/2017
DHS	DHS/ALL-042 Personnel Networking and Collaboration System	02/28/2018
DHS	DHS/ALL-011 Awards, Biographies, Professional Certifications or Licenses System of Records	04/05/2018
DHS	DHS/ALL-014 Personnel Contact Information	04/16/2018
DHS	DHS/ALL-041 External Biometric Records (EBR)	04/24/2018
DHS	DHS/ALL-039 Foreign Access Management System (FAMS)	05/01/2018
FEMA	DHS/FEMA-002 Quality Assurance Recording System (QARS)	07/14/2017
FEMA	DHS/FEMA-014 Hazard Mitigation Planning and Flood Mapping Products and Services Records	10/25/2017
ICE	DHS/ICE-013 Alien Health Records	03/19/2018
USCG	DHS/USCG-029 Notice of Arrival and Departure	07/17/2017
USCG	DHS/USCG-032 Asset Logistics Management Information System (ALMIS)	05/01/2018
USCIS	DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System	09/18/2017
USCIS	DHS/USCIS-012 Citizenship and Immigration Data Repository	05/01/2018
SORNs Rescinded During the Reporting Period		
USCIS	DHS/USCIS-014 Electronic Immigration System-1 Temporary Accounts and Draft Benefit Requests System	02/28/2018
USCIS	DHS/USCIS-015 Electronic Immigration System-2 Account and Case Management System	02/28/2018
USCIS	DHS/USCIS-016 Electronic Immigration System-3 Automated Background Functions System	02/28/2018