



Department of Homeland Security

2017 Privacy Office Annual Report to Congress

For the period July 1, 2016 – June 30, 2017

October 31, 2017



Homeland
Security

Message from the Chief Privacy Officer

October 31, 2017

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's *2017 Annual Report to Congress*, highlighting the achievements of the Privacy Office under the leadership of the former Acting Chief Privacy Officer, Jonathan A. Cantor, for the period July 2016 - June 2017.



I was appointed Chief Privacy Officer in July 2017, and was excited to take on this role because of the excellent reputation of both the Privacy Office and the privacy professionals throughout DHS. I look forward to continuing that history and contributing to the important mission of the Department.

The mission of the Privacy Office is more important today than ever before. In order to fulfill its vital national and public security mission, the Department needs to collect and share the personal information that is entrusted to us by the public. Thus, DHS is obligated by law and policy to ensure this information is properly collected, maintained, secured, and disseminated in order to maintain the integrity of that information, and mitigate against the adverse consequences resulting from a breach or misuse of data.

A robust privacy program – like any comprehensive risk management program – should help agency heads make informed policy decisions, use and share accurate and timely data more effectively, avoid risks, reduce costs, and improve the efficiency of government programs. A strategic privacy program led by capable experts helps *facilitate* technology and programmatic innovation, not slow it down.

Since its creation 13 years ago, the Privacy Office's goal has been to “operationalize” privacy throughout the Department. Privacy considerations are now woven directly into business processes throughout the Department to ensure that privacy is integrated into decision making from the very beginning.

We have built a robust privacy program by using a wide variety of policy, compliance, and educational tools that together implement the DHS Fair Information Practice Principles (FIPPs) across the Department. The FIPPs are the foundation for all privacy policy development and implementation at the Department, and must be considered whenever an operational or prospective DHS program or activity raises privacy concerns or involves the collection of Personally Identifiable Information (PII).

We want DHS personnel to understand and identify privacy risks, mitigate the risks, and proactively safeguard PII. Trust in government is critical, and protecting privacy is essential to maintaining that trust.

Please direct any inquiries about this report to the Privacy Office at 202-343-1717 or privacy@dhs.gov. This report and other information about the Privacy Office can be found on our website: www.dhs.gov/privacy.

Sincerely,

A handwritten signature in black ink, appearing to read "Philip S. Kaplan", is displayed within a light gray rectangular box.

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 John Conyers, Jr.

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 [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 strategic 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 *new* privacy and transparency policies:
 - [DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews](#) formalizes the Privacy Office's oversight responsibility to ensure that privacy protections are fully integrated into Component operations.
 - [DHS Privacy Policy Instruction 047-01-005 for Component Privacy Officers](#) requires all DHS Components to appoint a Privacy Officer to oversee privacy compliance, policy, and oversight activities in coordination with the CPO.

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.

-
- [*Freedom of Information Act Compliance Policy Directive 262-11*](#) defines the roles and responsibilities of the Chief FOIA Officer, the Deputy Chief FOIA Officer, Component FOIA Officers, and other responsible officials regarding FOIA.
 - Issued a *revised* privacy policy:
 - [*DHS Privacy Policy Guidance Memorandum 2017-01*](#). In response to Section 14 of Executive Order 13768, *Enhancing Public Safety in the Interior of the United States*, the Privacy Office rescinded its previous 2007 privacy policy (Privacy Policy Guidance Memorandum 2007-01/Privacy Policy Directive 262-12) titled *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*. To replace that policy and to clarify employee responsibilities under the several statutes that address the collection, use, retention, and dissemination of personal information, DHS issued a new policy on April 25, 2017 titled, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*.
 - 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 PII*](#):
 - **New:** *Privacy Incident Responsibilities and Breach Response Team*,² establishes the requirement for the Chief Privacy Officer to convene and lead a Breach Response Team (BRT) when a “major incident” that includes PII has occurred, or at the discretion of the Chief Privacy Office.
 - **Revised:** [*Privacy Incident Handling Guidance*](#), DHS’s breach response plan.
 - **Revised:** *Handbook for Safeguarding Sensitive PII*,³ a source of best practices to protect PII and prevent a privacy incident.
 - Issued an updated [FOIA regulation](#) to improve the management of the Department’s FOIA program.

Goal 2: Outreach, Education and Reporting

- Co-hosted the first-ever Privacy Talent Summit, bringing together over 200 human resource professionals and hiring managers to discuss ways to improve the recruiting and hiring of privacy professionals.
- Deployed new FOIA training:
 - *FOIA Training for Federal Employees*;
 - *FOIA Training for Professionals*; and a
 - Senior Executive Briefing video for agency senior executives.

Goal 3: Compliance and Oversight

- Approved 75 new or updated Privacy Impact Assessments, and 16 System of Records Notices, resulting in a Department-wide Federal Information Security Management Act privacy score of 94 percent for required investment technology system Privacy Impact Assessments, and 100 percent for System of Records Notices.

² To be published on DHS.gov in November 2017.

³ To be published on DHS.gov in November 2017.

-
- Published the [DHS 2016 Computer Matching Activity \(CMA\) Report](#), in which the DHS Data Integrity Board submitted a favorable cost benefit analysis for the overall program and reported the establishment of a new CMA between the Federal Emergency Management Agency and the United States Department of Housing and Urban Development that helped 2016 flood survivors and 2017 hurricane survivors receive benefits faster and more efficiently.
 - Completed three Privacy Compliance Reviews (PCR), oversaw implementation of recommendations from three previous PCRs, and launched four new PCRs.
 - Reviewed 585 raw intelligence information reports (IIR) and draft intelligence reports (FINTEL), 67 briefing packages, and 367 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 round-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 14 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 \$492,504 in reimbursable funding, which allowed us to direct more resources toward our privacy and FOIA support services contracts; and
- Conducted a review of our IT billing, data management and support requirements, resulting in an annual cost savings of \$245,000 for the Department.



Privacy Office

2017 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.....	23
Outreach.....	24
Education: Privacy & FOIA Training and Awareness.....	30
Reporting.....	32
III. Compliance & Oversight.....	33
Privacy Compliance.....	34
Information Sharing and Intelligence Activities	51
Privacy Incident and Complaint Handling	54
IV. Workforce Excellence	61
V. Component Privacy Programs.....	64
Federal Emergency Management Agency (FEMA)	65
National Protection and Programs Directorate (NPPD).....	68

Office of Intelligence and Analysis (I&A)	71
Science and Technology Directorate (S&T)	72
Transportation Security Administration (TSA).....	74
United States Citizenship and Immigration Services (USCIS)	76
United States Coast Guard (USCG).....	78
U.S. Customs and Border Protection (CBP)	80
United States Immigration and Customs Enforcement (ICE)	82
United States Secret Service (USSS or Secret Service).....	84
Appendix A – Acronyms	86
Appendix B – DHS Implementation of the Fair Information Practice Principles (FIPPs)....	89
Appendix C – Compliance Activities	90
Appendix D – Published PIAs and SORNs.....	93

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 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 (i) 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 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.⁴ All DHS systems, technology, and programs that either collect PII or have a privacy impact are subject to the oversight of the Chief Privacy Officer (CPO) and the requirements of U.S. data privacy laws.

Our expertise in privacy laws, both domestic and international, help us inform privacy policy development both within the Department and in collaboration with the rest of the Federal Government. Our office is responsible for evaluating Department programs, systems, and initiatives for potential privacy impacts, and providing mitigation strategies to reduce the privacy impact. We also advise senior leadership to ensure that privacy protections are implemented throughout the Department.

We are responsible for building a culture of privacy across the Department. We also train Department personnel on the importance of safeguarding privacy and complying with federal laws and privacy policies.

Who Do We Serve?

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

What Do We Do?

Our office aims to work with every Component and program in the Department to ensure that privacy considerations are addressed when *planning or updating* any program, system, or initiative. We strive to ensure that technologies used at the Department sustain, and do not erode, privacy protections. We also implement the Department's Fair Information Practice Principles (FIPPs) governing the use of personally identifiable information (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 Freedom of Information Act (FOIA) and Privacy Act operations and supports implementation across the Department;
- Operates a Department-wide Privacy Incident Response Program to ensure that breaches involving PII are properly reported, investigated, and mitigated, as appropriate;
- Responds to complaints of privacy violations and provides redress, as appropriate; and

⁴ Source: DHS Privacy Office FY 2015-2018 Strategic Plan. See hyperlink on page 11.

- Provides training, education, and outreach to build a culture of privacy across the Department and transparency to the public.

The Fair Information Practice Principles

The FIPPs,⁵ 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](#).

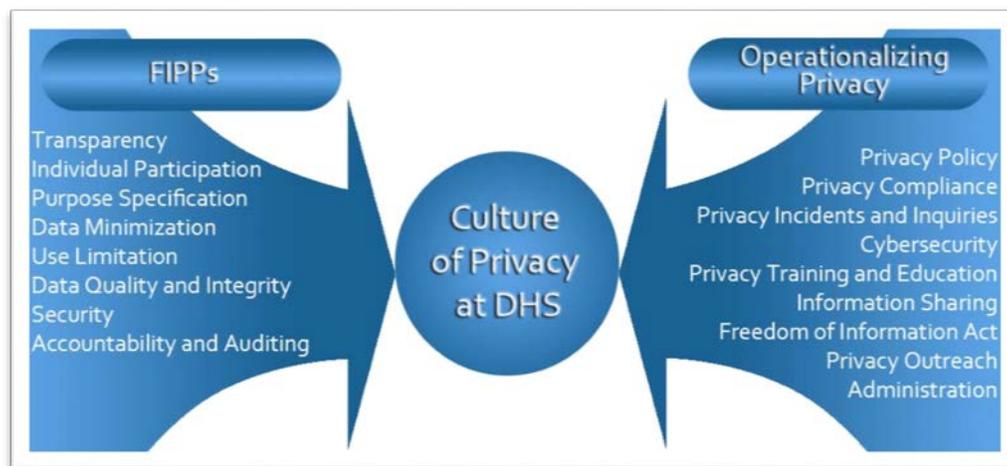


Figure 1: Privacy Office Implementation of the FIPPs

The Privacy Office incorporates these well-recognized principles into privacy and disclosure policy and compliance processes throughout the Department. We also undertake these statutory and policy-based responsibilities in collaboration with Component privacy officers,⁶ privacy points of contact (PPOC),⁷ Component FOIA Officers, and program offices to ensure that all privacy and disclosure issues are afforded the appropriate level of review and expertise.

For a detailed explanation of the FIPPs, please refer to Appendix B.

⁵ 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>

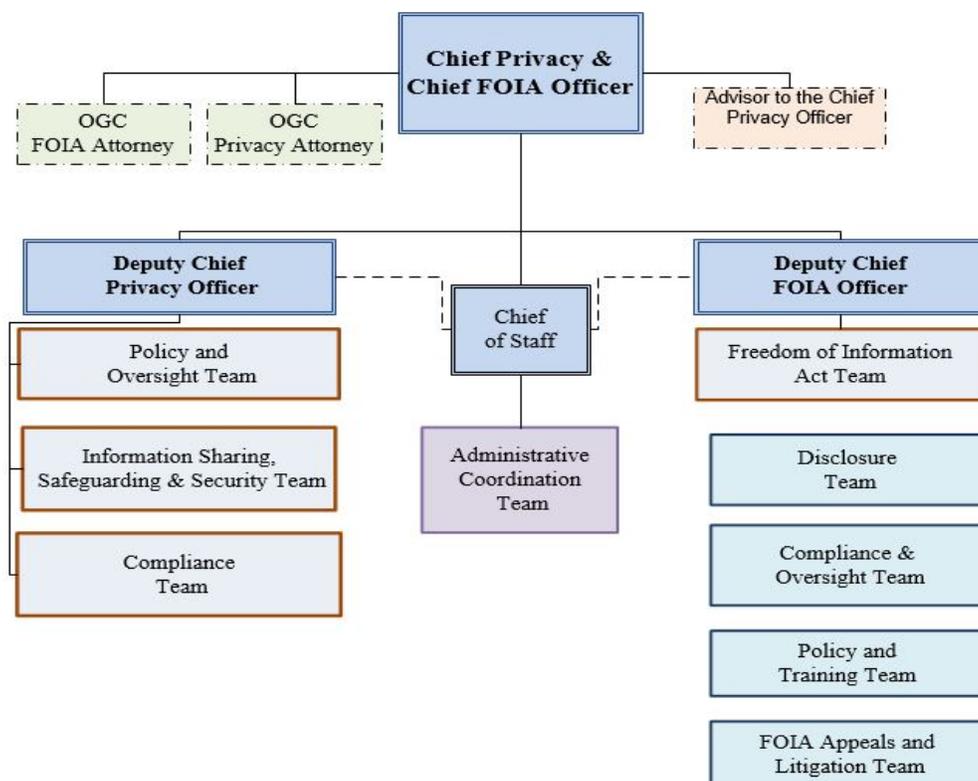
⁶ Every DHS Component is required by DHS policy to appoint a Privacy Officer to oversee privacy compliance, policy, and oversight activities in coordination with the CPO. See [DHS Privacy Policy Instruction 047-01-005, Component Privacy Officer](#).

⁷ 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.

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 “big data,” enterprise data management, cybersecurity, acquisitions and procurement, international engagement, and intelligence products. In addition, this team is dedicated to implementing accountability and continually improving DHS privacy processes and programs, in particular, the DHS Data Framework, which is DHS’s big data solution. 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 drafting 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 community and federal, state, local, tribal, territorial, and international law enforcement partners. The team engages with operational, policy, and oversight stakeholders—both within DHS and with the Interagency—throughout the information sharing lifecycle by evaluating information sharing requests, assessing and mitigating privacy risks, and reviewing compliance with agreement privacy terms and conditions over time. Team members participate in Privacy Office efforts to review intelligence products, provide intelligence-related privacy training, and provide policy guidance for other related DHS initiatives, including: safeguarding information and preventing insider threats, countering violent extremism, 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 coordinates Department-level compliance with FOIA by developing Departmental policy to implement important FOIA initiatives, including those set forth in applicable Department of Justice (DOJ) guidance. Additionally, the Privacy Office coordinates and oversees Component FOIA Office operations, provides FOIA training, and prepares 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
 - 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.

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 14 offices: Office of the Secretary, Office for Civil Rights and Civil Liberties, Office for Operations Coordination, Office for Community Partnerships, Office of the Citizenship and Immigration Services Ombudsman, Domestic Nuclear Detection Office, Office of the Executive Secretary, Office of Intergovernmental Affairs, Management Directorate, Office of Policy, Office of the General Counsel, Office of Health Affairs, Office of Legislative Affairs, and Office of Public Affairs.

How Can You Work With Us?

Department personnel:

- Partner with us when planning or updating any program, system, information sharing agreement, or initiative to ensure compliance with privacy law and policy;
- Know when to prepare privacy compliance documents;
- Educate yourself through our training programs on the proper handling of PII, and when and how to report a privacy incident; and
- Respond promptly to all requests for assistance from FOIA professionals.

Privacy community and the public:

- Contact us so we can respond to your privacy concerns or questions; and
- Participate in our workshops and educational opportunities.

International partners:

- Learn about the U.S. privacy framework;
- 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.





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 further 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 personal information. 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

- **NEW:** [*DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews*](#) implements DHS Directive 047-01, “Privacy Policy and Compliance,” with regard to the Component Head’s responsibility to assist the CPO in reviewing Component activities to ensure that privacy protections are fully integrated into Component operations.
- **NEW:** [*DHS Privacy Policy Instruction 047-01-005 for Component Privacy Officers*](#) requires all DHS Components to appoint a Privacy Officer to oversee privacy compliance, policy, and oversight activities in coordination with the CPO.
- **NEW:** [*Freedom of Information Act Compliance Policy Directive 262-11*](#) defines the roles and responsibilities of the Chief FOIA Officer, the Deputy Chief FOIA Officer, Component FOIA Officers, and other responsible officials regarding FOIA. The Privacy Office is developing instructions to supplement this directive to improve the Department’s compliance with FOIA and adherence to DHS FOIA policy.
- **UPDATED:** [*DHS Privacy Policy Guidance Memorandum 2017-01*](#). In response to Section 14 of Executive Order 13768, *Enhancing Public Safety in the Interior of the United States*, the Privacy Office rescinded its previous 2007 privacy policy (Privacy Policy Guidance Memorandum 2007-01/Privacy Policy Directive 262-12) titled *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*. To replace that policy and to clarify employee responsibilities under the several statutes that address the collection, use, retention, and dissemination of personal information, DHS issued a new policy on April 25, 2017 titled, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*. The new policy, consistent with the Privacy Act, explains that immigrants and non-immigrants,⁹ who are not subject to other legal protections (for example, the Judicial Redress Act of 2015), may only obtain access to their records through the Freedom of Information Act, and may not be granted amendment of their records upon request. The Executive Order restricts agency discretion to extend the rights and protections of the Privacy Act, subject to applicable law, beyond U.S. citizens and lawful permanent residents. The new 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).

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*](#), we issued one new privacy policy and two completely revised privacy policy instructions this year. For details, please see page 54.

⁹ A non-immigrant is an alien seeking temporary entry into the United States for a specific purpose.

-
1. New: *Privacy Incident Responsibilities and Breach Response Team*¹⁰
 2. Revised: [Privacy Incident Handling Guidance](#)
 3. Revised: *Handbook for Safeguarding Sensitive PII*¹¹

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. Where applicable, the related core DHS mission is indicated.

DHS Biometrics Strategic Framework

The Privacy Office continues to support the implementation of the DHS Biometrics Strategic Framework. As noted previously, the Privacy Office has relied upon the principles set forth in the [2011 Privacy Policy Guidance Memorandum, Roles & Responsibilities for Shared IT Services](#), to support the efforts of the Office of Policy (PLCY), Screening and Coordination Office (SCO), to build upon the adopted strategic framework and ensure a uniform DHS Biometrics Policy. The Privacy Office has concluded its coordination with both Headquarters and Component stakeholders regarding updates to the privacy compliance process for DHS's biometric holdings, and has prepared those documents for interagency review and publication to begin the transition of the new compliance framework. These documents inform not only the manner in which biometrics will be acquired and maintained, but also how biometrics will be used and shared with DHS partners. *Missions One – Five.*

Countering Violent Extremism (CVE)

The Privacy Office remains involved in the Department's CVE activities primarily through participation in the CVE Working Groups. We review proposed research and programs, along with work product, prior to completion to ensure that the Department's CVE work is consistent with applicable privacy law and policy. *Mission Number One: Prevent Terrorism and Enhance Security.*

Cybersecurity

The Privacy Office has an active role in the Department's cyber activities. We participated in the Under Secretary of the National Protection and Programs Directorate's (NPPD) weekly "Cyber Wednesday" meeting to discuss current activities in cybersecurity. We also support the drafting of privacy compliance documentation related to DHS cyber programs, and oversee the Data Privacy and Integrity Advisory Committee's cyber subcommittee. The Privacy Office also works heavily with NPPD on the Department's various cybersecurity initiatives, including



¹⁰ To be published on DHS.gov in November 2017.

¹¹ To be published on DHS.gov in November 2017.

the implementation of the Cybersecurity Information Sharing Act (CISA), the Automated Indicator Sharing (AIS) Initiative, the EINSTEIN programs, and all cyber-related Executive Order activities/deliverables under Executive Orders 13636, 13691, and 13800. As a part of this work, 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.*

Privacy Officer Review Required Under the Federal Cybersecurity Enhancement Act

The Federal Cybersecurity Enhancement Act Title II, Subtitle B, of the Cybersecurity Act of 2015 (FCEA) amended Section 230 (Federal Intrusion Detection and Prevention System) of the Homeland Security Act of 2002 to direct the CPO, in consultation with the Attorney General, to conduct a review of EINSTEIN policies and guidelines no later than one year after enactment. At the request of the CPO, NPPD Office of Privacy, and the NPPD Legal Division performed a privacy and legal analysis, respectively, of the Cybersecurity Information Handling Guidelines (CIHG) for consistency with the FIPPs and applicable privacy laws as required by the FCEA. These analyses were shared with the Department of Justice’s Office of Privacy and Civil Liberties pursuant to FCEA’s requirement to consult with the Attorney General.

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 concerns are identified and mitigated before any action or initiative is implemented.

Data Framework

DHS developed the Data Framework, 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 to build in privacy protections while enabling more controlled, effective, and efficient use of existing homeland security-related information across the DHS enterprise and with other U.S. Government partners, as appropriate. The Privacy Office continues to support the development of the Framework. The Data Framework, comprised of the Neptune and Cerberus Systems, 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 ensuring that robust policy and technical controls are in place to protect privacy. This year, the Data Framework continued its Initial Operational Capability (IOC) by 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. The Privacy Office serves a significant role as data sets 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 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 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 requirements generation process, harmonizes efforts across the Department, and makes prioritized funding recommendations to the DMAG for those validated 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. The Privacy Office provided significant support to two portfolio groups under the JRC: the Screening and Vetting Portfolio and the Information Sharing Portfolio Teams. These teams are responsible for evaluating various policy, resource, capability, or process issues, and providing recommendations to the JRC. *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 two separate interagency Federal Acquisition Regulation (FAR) efforts that have not been finalized:

1. The first is a FAR clause to implement the reporting requirements of OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information." When complete, this clause will require contractors and subcontractors that have access to, create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information on behalf of the Government, or operate an information system on behalf of the Government that may have personally identifiable information 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.
2. In addition, the Privacy Office is taking 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 will support this effort to ensure that sensitive information, including PII, is appropriately safeguarded throughout its lifecycle.

Freedom of Information Act (FOIA)

On June 30, 2016, former President Obama signed into law the FOIA Improvement Act of 2016¹² (the Act), which contains several substantive and procedural amendments to the FOIA, including new requirements. The Privacy Office has made significant strides in implementing each of the procedural amendments.

- To improve the implementation of the Act’s amendments, and to better operate as a policy and disclosure office, the Privacy Office’s FOIA function realigned into the following four concrete lines of business: FOIA disclosure, FOIA policy and training, FOIA compliance and oversight, and FOIA appeals and litigation.
- The Privacy Office finalized and issued the updated [FOIA regulation](#) to improve the management of the Department’s FOIA program. The regulation was published in the Federal Register on November 22, 2016, and became effective on December 22, 2016.
- On April 17, 2017, the Acting Under Secretary for Management signed the new [Directive 262-11](#), *Freedom of Information Act Compliance*, which clarified the roles and responsibilities of the Chief FOIA Officer, the Deputy Chief FOIA Officer, Component FOIA Officers, and other responsible officials regarding FOIA. The Privacy Office is developing instructions to supplement the directive to improve the Department’s compliance with FOIA and adherence to DHS FOIA policy.
- Additionally, during the reporting period, the Privacy Office and six Components implemented the recommendations that the Office of Government Information Services (OGIS) provided in response to [OGIS’s Compliance Reports](#) regarding FOIA policies, procedures, and compliance.

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. On May 18, 2017, the former Acting CPO approved the Wyoming Information and Analysis Team (WIAT) Privacy, Civil Rights, and Civil Liberties Policy. Wyoming’s policy is the 79th fusion center “privacy” policy to be found—in keeping with the requirements of the *Guidelines to Ensure that Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment* (“ISE Privacy Guidelines”)—“at least as comprehensive” as the ISE Privacy Guidelines. The Privacy Office worked with the I&A State and Local Liaison, I&A Field Operations, and the WIAT management team to efficiently resolve suggested edits so that the policy could quickly be made available to the public on the WIAT

¹² FOIA Improvement Act of 2016 (Public Law No. 114-185).

website. The Privacy Office provided additional significant support for the development of the *Real-Time and Open Source Analysis Resource Guide*, the *Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development Template and Guidance*, and the forthcoming *Face Recognition Policy Development Template*. **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 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.

Screening and Vetting Initiatives

To identify and mitigate privacy concerns that may arise from implementation of President Trump's March 6, 2017 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. As a part of this work, the DHS Privacy Office is a member of the DHS Shared Services for Vetting Board, which seeks to define and develop how the Department vets travelers. This group has a high level of participation across the Department, and the Privacy Office is engaged as a full-time voting member. **Mission Number One: Prevent Terrorism and Enhance Security.**

Social Media Task Force

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



DHS uses social media for four purposes:

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 significant risks to privacy. Because of this, the Privacy Office is working 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. *Missions One and Two: Prevent Terrorism, Enhance Security, and Secure and Manage Our Borders.*

Unmanned Aircraft Systems: DHS Privacy, Civil Rights, and Civil Liberties Working Group on UAS¹³

The Privacy Office is active in several aspects of the Department's employment or support of unmanned aircraft systems (UAS). Indeed, all Privacy Office teams play some role in either 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), or developing policies and procedures to help counter threats to the Homeland from the use of UAS by our adversaries.



Whenever the Components consider the acquisition, development, or deployment of UAS, they must first complete a PTA. Most of the PTAs regarding UAS that the Privacy Office reviews are for 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

¹³ Memorandum For The Secretary from Tamara J. Kessler, Acting Officer for Civil Rights and Civil Liberties and Jonathan R. Cantor, Acting Chief Privacy Officer, "Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department's Use and Support of Unmanned Aerial Systems (UAS)" September 14, 2012, <https://www.dhs.gov/sites/default/files/publications/foia/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-s1-information-memorandum-09142012.pdf>.

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 on the Internet 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 the CRCL to evaluate grant applications from SLTT agencies received by the FEMA Grant Programs Directorate, 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 five such applications during the current reporting period. One is currently on hold pending submission of additional material at the request of the Privacy Office, one was cleared after submitting additional material, and the Privacy Office has cleared the other three without requiring anything additional. In all cases, we provide applicants with links to the “DHS UAS Best Practices” cited below 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 may be a 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 a DHS Component might inappropriately gain access to a person’s PII. This is an ongoing project that is likely to be completed during the next reporting period.

The Privacy Office co-chairs the DHS Working Group on UAS, which was created to provide a forum for all DHS Components whose work relates in some way to UAS activities to discuss items of common interest, and to coordinate guidance on privacy, civil rights, and civil liberties issues. The Working Group published the DHS [*Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft Systems Programs*](#) in December 2015. These best practices reflect the lessons learned through the Department’s operation of UAS, and may be used by any Component whose future plans include funding or deploying UAS. They may also inform state and local law enforcement agencies about issues to consider when establishing a UAS program. *Mission Number Two: Secure and Manage Our Borders.*



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 regularly looks for ways to promote transparency and engage with the privacy advocacy community, international partners and stakeholders, and the public. Methods of engagement include public workshops, DHS blog postings, the Privacy Office website, the Federal Privacy Council's Federal Privacy Summit, and Privacy Office leadership and staff appearances at conferences and other forums. 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 policies and best practices.

- ***American Society of Access Professionals Ninth National Training Conference*** – On July 19, 2016, in Arlington, Virginia, the former Acting CPO participated in a panel discussion, *Flex Your Privacy Muscle: How to Strengthen Your Privacy Program*.
- ***Privacy Talent Summit*** – On September 14, 2016, in Washington, DC, the Federal Privacy Council hosted the first-ever Privacy Talent Summit, which brought together over 200 human resources professionals and hiring managers to discuss ways to improve recruitment and hiring of privacy professionals. The Federal Privacy Council developed a “toolkit” with resources to help human resources and hiring managers as they make decisions about which types of positions they should use in their privacy offices, design federal privacy positions, then conduct recruitment and selection activities. The former Acting CPO is a co-chair of the Subcommittee leading this effort.
- ***Federal Privacy Summit*** – On November 10, 2016, in Washington, DC, the Federal Privacy Council hosted a one-day workshop that convened privacy, technology, budget, procurement, human resources, public affairs, congressional affairs, and intergovernmental affairs staff from many federal agencies to discuss privacy and security. Subject matter experts, including the former Acting CPO, shared best practices for protecting privacy, and ways to improve collaboration across the enterprise. The keynote speaker was the former Senior Advisor to the OMB Director. The former Acting CPO and other members of the Privacy Office participated as panelists in several breakout sessions.
- ***FedScoop’s Federal Executive Leadership Roundtable on Emerging Technology*** – On December 1, 2016, in Washington, DC, the former Acting CPO joined other government panelists to discuss emerging technology in the public sector.
- ***The International Association of Privacy Professionals (IAPP) Practical Privacy Series*** – On December 8, 2016, in Washington, DC, the former Acting CPO hosted a one-day workshop on technology issues facing public sector privacy professionals. The keynote speaker was the former Senior Advisor to the OMB Director.
- ***U.S. Department of Health and Human Services (HHS) Data Privacy Day Workshop*** – On January 26, 2017, in Washington, DC, the HHS Privacy Director moderated a panel of privacy experts to discuss the past, present, and future of privacy in the Federal Government.
- ***The IAPP Global Summit*** – On April 20, 2017, in Washington, DC, the former Acting CPO moderated a panel on Privacy Compliance Reviews comprising the DHS Director of Privacy Oversight and Christopher Pierson, a member of the DHS Data Privacy and Integrity Advisory Committee.

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. During the reporting period, the Privacy Office engaged in the following FOIA outreach activities:

- The Chief FOIA Officer and the Deputy Chief FOIA Officer are members of the Chief FOIA Officer Council¹⁴ 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.
- In October 2016, the Privacy Office Director of Appeals and Litigation served on a panel titled *FOIA Litigation from the Processor's Perspective* at the Department of Justice's (DOJ) Office of Information Privacy (OIP) FOIA Litigation Seminar. The panelists provided best practices for FOIA professionals to interact with the litigation process.

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:

- **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 experience needed in today's tech-driven and big data environment; hiring the right people at

¹⁴ 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.

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. As mentioned earlier, on September 14, 2016, this Committee hosted the first-ever Privacy Talent Summit, which brought together over 200 human resources professionals and hiring managers to discuss ways to improve recruiting and hiring of privacy professionals.

- **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 myriad 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 designed and twice delivered an eight-week Privacy Bootcamp 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.¹⁵ 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.

¹⁵ 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.

Members hold public meetings to receive updates from the Privacy Office on important privacy issues, and to deliberate taskings from the CPO.

- On February 21, 2017, the Privacy Office hosted a virtual public meeting of the DPIAC where the members deliberated, voted on, and subsequently issued their [*Report 2017-01, Best Practices for Notifying Affected Individuals of a Large-Scale Data Breach*](#).

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.

- On August 1, 2017, at U.S. Customs and Border Protection (CBP) Headquarters in Washington, D.C., DHS Deputy CPO, Jonathan Cantor, and CBP Deputy Executive Assistant Commissioner of Field Operations, John Wagner, 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. *See page 80 for more information on this program.*

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), is supporting 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; the oversight includes the system rules for permitting access to information, the system's analytical capabilities, including data mining, and any related dissemination of information. The review is focusing on the use of datasets that are already incorporated into the system and the 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*.

Congressional Outreach

Congressional Testimony

The Chief Privacy Officer did not testify at any congressional hearings during the reporting period. Historical written testimony can be found on the Privacy Office website:

www.dhs.gov/privacy.

Congressional Staff Briefings

Privacy Office staff, including the Chief Privacy Officer, briefed Congress several times during the reporting period on a range of issues.

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 programs to share PII or establish privacy best practices, the Privacy Office provides expertise 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 13 representatives from 10 countries (see chart on next page). These engagements included briefings on the U.S. privacy and FOIA frameworks, DHS privacy and disclosure policy, privacy compliance documentation, and privacy and information sharing. By advancing DHS privacy compliance and policy practices to international partners and promoting the FIPPs, the Privacy Office pushes out DHS 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 “DHS 201,” a week-long training course for new DHS attachés being deployed to U.S. embassies worldwide by providing an international privacy policy module to raise awareness of the potential impact of global privacy policies on participant’s work.

Figure 3: International Engagements

INTERNATIONAL ENGAGEMENTS			
DATE	COUNTRY	ORGANIZATION	TOPICS
September 2016	Canada	Immigration, Refugees, And Citizenship Canada	U.S. Policies and Legislation Related to Data Privacy and Protection
February 2017	Vietnam	Hue University	General Privacy, Incidents, Cyber
February 2017	Philippines	IT and Business Process Association of the Philippines	General Privacy, Incidents, Cyber

INTERNATIONAL ENGAGEMENTS			
DATE	COUNTRY	ORGANIZATION	TOPICS
February 2017	Thailand	INTERPOL Thailand	General Privacy, Incidents, Cyber
February 2017	Malaysia	Malaysian Communications and Multimedia Commission	General Privacy, Incidents, Cyber
February 2017	China	Watching Media	General Privacy, Incidents, Cyber
April 2017	New Zealand	Office of Privacy Commissioner	General Privacy
May 2017	Germany	Radio Station "Detektor.Fm"	General Privacy, EO, Border Searches, Cyber
May 2017	Germany	Bavarian Data Protection Authority	General Privacy, EO, Border Searches, Cyber
May 2017	Germany	Digital Mitteldeutsche Zeitung	General Privacy, EO, Border Searches, Cyber
June 2017	Malta	United Nations Office of the High Commissioner for Human Rights	U.S. and European Surveillance Safeguards
June 2017	Spain	United Nations Office of the High Commissioner for Human Rights	U.S. and European Surveillance Safeguards
June 2017	Germany	The University of Groningen	U.S. and European Surveillance Safeguards

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.”¹⁶ The Privacy Office and the Component FOIA Offices conduct internal training to agency staff 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.

¹⁶ 5 U.S.C. § 552 (j)(2)(F).

In addition to conducting training, the Privacy Office also provides training materials to agency staff regarding their responsibilities under the FOIA. During the reporting period, the Privacy Office deployed the DOJ's Office of Information Policy (OIP) FOIA training listed below Department-wide through the online learning systems:

- In October 2016, the Privacy Office deployed *FOIA Training for Federal Employees*. This training provides a primer on the FOIA, and highlights ways to assist agencies in administering the FOIA law. It is a good reminder that FOIA is everyone's responsibility.
- In June 2017, the Privacy Office deployed *FOIA Training for Professionals*. This in-depth training addresses all the major procedural and substantive requirements of the law, as well as the importance of customer service.
- In June 2017, the Privacy Office deployed the Senior Executive Briefing video for agency senior executives, providing a general overview of the FOIA and emphasizing the importance of their support to the agency's FOIA program.



Reporting

The Privacy Office issues congressionally-mandated public reports, including this one, that document progress in implementing DHS privacy and FOIA policy. During the reporting period, the Privacy Office issued the following reports, which can be found on the Privacy Office website under Privacy and FOIA Reports: www.dhs.gov/privacy.

- ***Privacy Office Semi-Annual Report to Congress:*** The Privacy Office issues two semi-annual reports to Congress as required by Section 803 of the 9/11 Commission Act,¹⁷ 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 for responding to requests, increases proactive disclosures, fully utilizes technology, reduces backlogs, and improves 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 2007¹⁸ definition of data mining.
- ***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.

¹⁷ 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.

¹⁸ 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 assesses the privacy risk of Departmental programs and develop mitigation strategies by reviewing and approving all DHS privacy compliance documentation.

The DHS privacy compliance documentation process 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)¹⁹ privacy reporting.

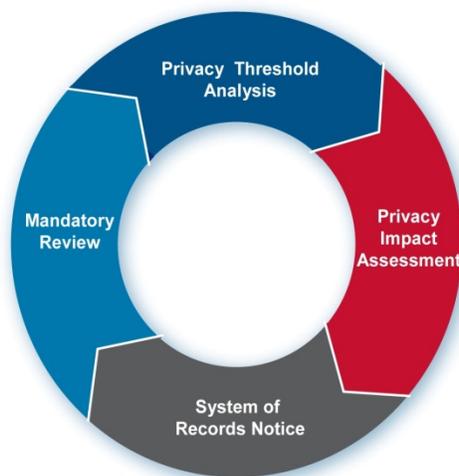


Figure 4: Privacy Office Compliance Process

¹⁹ 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 2017, the Department’s FISMA privacy score showed that 94 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 100 percent of required SORNs had 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 75 PIAs, and a complete list by Component can be found in Appendix D.

Listed here are 11 key PIAs approved during this reporting period:

1. [DHS/CBP/PIA-021 TECS System: Platform](#)

Background: The TECS Platform facilitates information sharing among federal, state, local, and tribal government agencies, as well as with international governments and commercial organizations. CBP’s mission includes the enforcement of the customs, immigration, and agriculture laws and regulations of the United States and the enforcement at the border of hundreds of laws on behalf of numerous federal agencies. Through the TECS Platform, users are able to input, access, or maintain law enforcement, inspection, intelligence-gathering, and operational records.

Purpose: CBP published this PIA as a complement to the previously published DHS/CBP/PIA-009, CBP Primary and Secondary Processing PIA from 2010, to provide notice to the public and to assess the privacy risks and mitigations associated with the TECS Platform. (*August 12, 2016*)

2. [DHS/ALL/PIA-058 Access Lifecycle Management](#)

Background: DHS Access Lifecycle Management (ALM) is the technology and business process that manages the identities and access rights of DHS employees and contractors, ensuring that they only have access to approved systems and applications.

Purpose: DHS published this PIA because ALM uses, stores, and disseminates PII of DHS employees and contractors in order to manage their accounts and identities. (*January 24, 2017*)

3. [DHS/CBP/PIA-032 Human Resources Business Engine \(HRBE\)](#)

Background: CBP provides Human Resources (HR) services to CBP and other DHS components through a web-based tool called the Human Resources Business Engine (HRBE). HRBE provides case management and HR business process capabilities to CBP and its DHS component customers. The specific HR services vary based on the need and service request of each DHS component customer.

Purpose: CBP conducted this PIA because HRBE collects, uses, maintains, and disseminates PII belonging to members of the public and because HRBE provides HR services to multiple DHS components with plans to further expand within the DHS enterprise. *(July 25, 2016)*

4. [DHS/FEMA/PIA-045 Hazard Mitigation Planning and Flood Mapping Products and Services Support Systems](#)

Background: Federal Emergency Management Agency (FEMA)'s Federal Insurance and Mitigation Administration (FIMA) provides various flood mapping products and services to the public as required under the National Flood Insurance Act of 1968, as amended (NFIA) (42 U.S.C. § 4001 et seq.). The Risk Management Directorate (RMD) manages FIMA's various flood mapping products and services. This includes the Map Service Center (MSC) and the Mapping Information Platform (MIP) IT support systems.

Purpose: FEMA updated and replaced the previously published DHS/FEMA/PIA-007 and DHS/FEMA/PIA-028, originally published April 30, 2013, to provide more detail about the MIP process, describing additional collections, use of financial information, the sharing of information with the Department of Treasury, and the development of the online Letter of Map Change (LOMC) application within MIP. *(June 26, 2017)*

5. [DHS/USCIS/PIA-009 Central Index System](#)

Background: United States Citizenship and Immigration Services (USCIS) maintains the Central Index System (CIS). CIS contains information on the status of applicants and petitioners seeking immigrant and non-immigrant benefits to include: lawful permanent residents, naturalized citizens, United States border crossers, aliens who illegally entered the United States, aliens who have been issued employment authorization documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the Immigration and Nationality Act (INA).

Purpose: USCIS updated and reissued the CIS PIA to clarify CIS's functionalities and to update the systems interconnected to CIS. *(April 13, 2017)*

6. [DHS/CBP/PIA-033 Electronic Visa Update System](#)

Background: CBP's Electronic Visa Update System (EVUS) is a web-based enrollment system used to collect information from nonimmigrant aliens who 1) hold a passport that was issued by an identified country approved for inclusion in the EVUS program and 2) have been issued a U.S. nonimmigrant visa of a designated category. EVUS, similar to the Electronic System for Travel Authorization (ESTA) program, collects updated information in advance of an individual's travel to the United States. EVUS also enables DHS to collect updated information from designated travelers during the interim period between visa applications.

Purpose: CBP published this PIA because EVUS is a new system that collects and uses personally identifiable information from individuals who meet the EVUS programmatic criteria,

as well as information of U.S. citizens identified on the EVUS enrollment request (*August 25, 2016*)

7. DHS/CBP/PIA-007(g) Electronic System for Travel Authorization

Background: The Electronic System for Travel Authorization (ESTA) is a web-based application and screening system used to determine whether citizens and nationals from countries participating in the Visa Waiver Program (VWP) are eligible to travel to the United States.

Purpose: DHS/CBP published this update to the PIA for ESTA, last updated on June 20, 2016, to provide notice and assess the privacy risks associated with recent enhancements to the ESTA application questionnaire, including the addition of an optional field for social media usernames or identifiers for all ESTA applicants. (*September 1, 2016*)

8. DHS/NPPD/PIA-030 Continuous Diagnostics and Mitigation

Background: NPPD's Office of Cybersecurity and Communications (CS&C) developed the Continuous Diagnostics and Mitigation (CDM) program to support Government-wide and agency-specific efforts to implement adequate, risk-based, and cost-effective cybersecurity. CDM provides continuous monitoring, diagnostics, and mitigation services designed to strengthen the security posture of participating federal civilian departments and agencies' systems and networks through the establishment of a suite of capabilities that enables network administrators to know the state of their respective networks at any given time, informs Chief Information Officers (CIO) and Chief Information Security Officers (CISO) on the relative risks of threats, and makes it possible for Government personnel to identify and mitigate vulnerabilities.

Purpose: NPPD conducted this PIA to cover the first three phases of the program, and address privacy risks associated with CS&C's deployment and operation of the CDM Federal Dashboard. (*September 30, 2016*)

9. DHS/ICE/PIA-047 DHS Victim Information and Notification Exchange

Background: The DHS Information and Notification Exchange (DHS-VINE) is a system that DHS U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO) established to automatically notify certain individuals about changes to a particular alien's custodial status with ICE. Notifications are sent about aliens who have been convicted of or charged with a crime, so long as a crime victim or victim advocate has registered with DHS-VINE to be notified upon change to the alien's custodial status with ICE. For purposes of the DHS-VINE system, individuals eligible to receive custody status notifications – hereafter “eligible registrants” – are victims and witnesses associated with aliens charged or convicted of a crime (at the federal or state level), as well as “victim advocates.” Victim advocates are individuals with a legal responsibility to act on behalf of a victim or witness (e.g., attorneys, parents, and legal guardians) and individuals acting at the request of a victim or witness. DHS-VINE will allow eligible registrants to directly register for custodial status notifications via a

web interface, and will also transfer eligible registrant data from a state VINE database to ensure those individuals who registered to receive state notifications continue to receive custody status updates once an alien is transferred from state to ICE custody.

Purpose: This PIA details the protections that are in place for the PII pertaining to eligible registrants and aliens that DHS-VINE collects, uses, and maintains. *(January 10, 2017)*

10. DHS/CBP/PIA-006(e) Automated Targeting System

Background: CBP operates the Automated Targeting System (ATS). ATS is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments.

Purpose: CBP updated this PIA to notify the public about ATS user interface enhancements for passenger vetting (known as Unified Passenger or UPAX), the use of ATS for vetting new populations, vetting of master crew member list and master non-crew member list data, collected under 19 C.F.R. § 122.49c, and several new information sharing initiatives, including between the Transportation Security Administration (TSA) and CBP to enhance the identification of possible threats and to enhance border and transportation security. *(January 13, 2017)*

11. DHS/ALL/PIA-059 DHS Employee Collaboration Tools

Background: DHS employs various cloud-based services and employee collaboration tools to promote efficiency and improve content management and employee communication across the enterprise. DHS cloud-based services and tools are used by departmental programs that do not have other content tracking systems to more effectively and efficiently manage the receipt, creation, assignment, tracking, and storage of agency matters.

Purpose: DHS conducted this PIA because cloud-based content management solutions and employee collaboration tools collect, use, store, and disseminate PII and Sensitive PII. This PIA replaced two previous DHS PIAs: DHS/ALL/PIA-023 DHS IdeaFactory (January 21, 2010) and DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites (March 22, 2011). *(February 7, 2017)*

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 16 SORNs, and a complete list by Component can be found in Appendix D.

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

1. DHS/ALL-014 Personnel Emergency Contact Information System of Records

Background: This system of records allows DHS to collect and maintain necessary records concerning DHS personnel (including federal employees and contractors) for workforce accountability. The system also includes records of federal employees, contractors, or other individuals who participate in or who respond to all-hazards emergencies including technical, manmade, or natural disasters, or who participate in emergency response training exercises; and individuals identified as emergency points of contact.

Purpose: The purpose of this system is for DHS workforce accountability, to support DHS all-hazards emergency response deployments and exercises, and to contact designated persons in the event of an emergency. As a result of a biennial review of this system, DHS updated this system of records notice to include several changes, including: system name, categories of individuals, categories of records, authority for maintenance, purpose, and retention and disposal. Additionally, this notice included non-substantive changes to simplify the formatting and text of the previously published notice. (*August 25, 2016, 81 FR 48832*)

2. DHS/ICE-016 FALCON Search and Analysis System of Records

Background: FALCON Search and Analysis is a consolidated information management system that enables ICE law enforcement and homeland security personnel to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws.

Purpose: The purpose of this system of records is to permit ICE law enforcement and homeland security personnel to search, aggregate, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal and administrative laws. FALCON-SA allows ICE HSI agents, criminal research specialists, and intelligence analysts to conduct research in order to produce law enforcement intelligence, provide lead information for investigative inquiry and follow-up, assist in ICE investigations and the disruption of criminal (including terrorist) activity, and discover previously unknown connections among ICE investigations. This system of records also supports the operation of the agency's Tip Line to collect, analyze, and act on information volunteered by the public and other sources concerning suspicious and potentially illegal activity. In addition to supporting the identification of potential criminal activity, immigration violations, and threats to homeland security, the system is also used to uphold and enforce the law, and to ensure public safety. (*May 4, 2017, 82 FR 20905*)

3. DHS/USCG-031 USCG Law Enforcement (ULE) System of Records

Background: This system of records allows the United States Coast Guard (USCG) to collect and maintain records related to maritime law enforcement, marine environmental protection, and the determinations supporting enforcement action taken by the USCG.

Purpose: The purpose of this system is to collect and maintain USCG case records and other reported information relating to the safety, security, law enforcement, environmental, and compliance activities of vessels, facilities, and organizations engaged in marine transportation, and related persons. (*December 8, 2016, 81 FR 88697*)

4. DHS/CBP-022 Electronic Visa Update System (EVUS) System of Records

Background: This system of records allows CBP to collect and maintain records on nonimmigrant aliens who hold a passport that was issued by an identified country approved for inclusion in the EVUS program and have been issued a U.S. nonimmigrant visa of a designated category seeking to travel to the United States. The system of records also covers records of other persons, including U.S. citizens and lawful permanent residents, whose name is provided to DHS as part of a nonimmigrant alien's EVUS enrollment. Requiring aliens holding passports of identified countries containing U.S. nonimmigrant visas of a designated category with multiple year validity will allow CBP to collect updated information. The system is used to ensure a visa holder's information remains current. The information is also used to separately determine whether any admissibility issues may need to be addressed outside the EVUS enrollment process by vetting the information against selected security and law enforcement databases at DHS, including the use of CBP's TECS (not an acronym) (CBP-011 U.S. Customs and Border Protection TECS, December 19, 2008, 73 FR 77778) and the Automated Targeting System (ATS) (DHS/CBP-006 Automated Targeting System, May 22, 2012, 77 FR 30297). In addition, ATS retains a copy of EVUS enrollment data to identify EVUS enrollees who may pose a security risk to the United States. The ATS maintains copies of key elements of certain databases in order to minimize the impact of processing searches on the operational systems and to act as a backup for certain operational systems. DHS may also vet EVUS enrollment information against security and law enforcement databases at other federal agencies to enhance DHS's ability to determine whether the enrollee poses a security risk to the United States or, although addressed through a separate process, is admissible to the United States. The results of this vetting may inform DHS's assessment of whether the enrollee's travel poses a law enforcement or security risk, and whether the proposed travel should be permitted.

Purpose: The purpose of this system is to collect and maintain a record of nonimmigrant aliens holding a passport issued by an identified country containing a U.S. nonimmigrant visa of a designated category, and to determine whether there is information that requires separate, additional action. (*September 1, 2016, 81 FR 60371*)

5. DHS/USCIS-007 Benefit Information System

Background: USCIS collects, uses, and maintains the Benefit Information System records to process and adjudicate immigrant or nonimmigrant benefit requests, “hereinafter collectively referred to as “benefit requests.” Benefit requests are submitted for naturalization, lawful permanent residence, asylum, refugee status, and other immigrant and nonimmigrant benefits in accordance with U.S. immigration law. USCIS also uses the Benefit Information System to support national security by preventing individuals from fraudulently obtaining immigration benefits and by denying benefit requests submitted by individuals who pose national security or public safety threats.

Purpose: USCIS updated this system of records to: (1) Update the system location to include international offices and replicated copies on unclassified and classified networks; (2) update the category of individuals to include interpreters, preparers, physicians, and sponsors; (3) expand the categories of records to clarify the data elements that USCIS collects from benefit requestors, beneficiaries, and family members; benefit sponsors; representatives; preparers and interpreters; and physicians; (4) separate routine use (N) into two separate routine uses (i.e., (N), (O)) to provide clarity on information sharing with federal, state, tribal, or local government agencies and foreign government agencies for the repayment of loans; (5) update routine uses (W), (X), (Y), and (Z) to permit the sharing of information pursuant to a Computer Matching Agreement, or other agreement with the Department of Labor, with the public during the course of naturalization ceremonies, and with the Department of Treasury, respectively; (6) update retention schedules for each record type; (7) expand data elements used to retrieve records from the elements listed or a combination thereof; (8) update sources of records to include interpreters, preparers, and physicians; and (9) expand the system classification to provide notice that Benefit Information System records may be stored on both DHS unclassified and classified networks to allow for analysis and vetting consistent with existing USCIS authorities and purposes and this published notice. Additionally, this notice included non-substantive changes to simplify the formatting and text of the previously published notice. (*October 19, 2016, 81 FR 72069*)

6. DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records

Background: DHS updated, renamed, and reissued a DHS system of records titled, “DHS//ICE-011 Immigration and Enforcement Operational Records (ENFORCE)” system of records. ICE collects, uses, and maintains ENFORCE to support the identification, apprehension, and removal of individuals unlawfully entering or present in the United States in violation of the Immigration and Nationality Act, including fugitive aliens. ICE also uses ENFORCE to support the identification and arrest of individuals (both citizens and non-citizens) who commit violations of federal criminal laws enforced by DHS. This system of records is being created from a previously issued system of records, DHS/ICE 011-Immigration and Enforcement Operational Records (ENFORCE). *See* 80 FR 24,269 (Apr. 30, 2015).

Purpose: ICE updated this system of records to: Change the system of records name to “DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER)” System of Records; update and reorganize the categories of individuals for clarity; expand the

categories of records to include recordings of detainee telephone calls and information about these calls, as well as information related to detainees' accounts for telephone or commissary services in a detention facility; update the system manager; clarify system location; and add twenty-five routine uses and modify twenty routine uses to describe how the Department of Homeland Security may share information from this system. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. (*October 19, 2016, 81 FR 72080*)

7. DHS/CBP-009 Electronic System for Travel Authorization (ESTA) System of Records

Background: This system of records allows CBP to collect and maintain records on nonimmigrant aliens seeking to travel to the United States under the Visa Waiver Program and other persons, including U.S. citizens and lawful permanent residents, whose names are provided to DHS as part of a nonimmigrant alien's ESTA application or Form I-94W. The system is used to determine whether an applicant is eligible to travel to and enter the United States under the Visa Waiver Program (VWP) by vetting his or her ESTA application information or Form I-94W information against selected security and law enforcement databases at DHS, including TECS (not an acronym) and the Automated Targeting System (ATS). In addition, ATS retains a copy of ESTA application and Form I-94W data to identify individuals from Visa Waiver Program countries who may pose a security risk to the United States. The ATS maintains copies of key elements of certain databases in order to minimize the impact of processing searches on the operational systems and to act as a backup for certain operational systems. DHS may also vet ESTA application information against security and law enforcement databases at other federal agencies to enhance DHS's ability to determine whether the applicant poses a security risk to the United States and is eligible to travel to and enter the United States under the VWP. The results of this vetting may inform DHS's assessment of whether the applicant's travel poses a law enforcement or security risk and whether the application should be approved.

Purpose: The purpose of this system is to collect and maintain a record of persons who want to travel to the United States under the VWP, and to determine whether applicants are eligible to travel to and enter the United States under the VWP. CBP updated this system of records notice, to clarify the category of individuals, expand a routine use, and expand the record source categories to include information collected from publicly available sources, such as social media. (*September 2, 2016, 81 FR 60713*)

8. DHS/CBP-023 Border Patrol Enforcement Records (BPER) System of Records

Background: This system of records contains information CBP collects and maintains to secure the U.S. border between the Ports of Entry (POE), furthering its enforcement and immigration mission.

Purpose: CBP issued this new system of records to claim ownership of records created as a result of CBP interactions between the POE. CBP inputs non-intelligence information it collects as a result of these interactions into its E3 Portal. CBP also collects and maintains information related to camera and sensor alerts in its Intelligent Computer Assisted Detection (ICAD) database. This system of records applies to the categories of information input and maintained in

these systems. This information includes biographic, biometric, geolocation imagery and coordinates, and other enforcement and detention data associated with encounters, investigations, border violence, seized property in relation to an apprehension, inspections, prosecutions, and custody operations of CBP between the ports of entry for law enforcement, immigration, or border security purposes. (*October 20, 2016, 81 FR 72601*)

Privacy Compliance Reviews

The Privacy Office exercises its oversight function under Section 222 of the Homeland Security Act to assure that the Department's use of technology sustains and does not erode privacy protections,²⁰ primarily by conducting Privacy Compliance Reviews (PCR). PCRs are a *constructive and collaborative* mechanism to assess implementation of protections described in PIAs, SORNs, or Information Sharing Access Agreements (ISAA), to identify areas for improvement, and to correct course if necessary. PCRs are distinct from the CPO's investigative authority.



The PCR framework emphasizes transparency 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.

The Privacy Office created [Standard Operating Procedures](#) to conduct PCRs in November of 2016 and issued [DHS Privacy Policy Instruction 047-01-004](#) for PCRs on January 19, 2017; this instruction elaborated the Component Head's responsibility to assist the CPO in reviewing Component activities to ensure that privacy protections are fully integrated into Component operations.

PCRs may result in public reports or internal recommendations, depending upon the sensitivity of the program under 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, oversaw implementation of recommendations from three previous PCRs, and launched four new PCRs.

²⁰ 6 U.S.C. § 142(a)(1).

PCRs Completed

[Enhanced Cybersecurity Services \(ECS\) Program, July 18, 2016](#)

ECS is a voluntary DHS program in which NPPD's Office of Cybersecurity and Communications provides indicators of malicious cyber activity to participating commercial service providers. The purpose of the program is to assist the owners and operators of critical infrastructure in enhancing their ability to protect their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program.

On April 10, 2015, the Privacy Office finalized its PCR of NPPD's ECS program, which found that NPPD developed the ECS Program and its related processes with privacy-protective objectives in mind. The 2015 PCR recommendations included making updates to the ECS PIA to augment NPPD's existing transparency efforts, and addressing changes in the program as it matured. The ECS PIA was updated on November 30, 2015, which addressed the four PCR recommendations.

Based on the ECS PIA update, as well as information provided in the July 2016 Executive Order 13636 Privacy and Civil Liberties Assessment Report, the Privacy Office found that NPPD continues to operate the ECS Program and its related processes with strong privacy oversight. The Privacy Office considers the 2015 PCR recommendations fully implemented and considers the 2016 PCR closed.

[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.

Due to the sensitive nature of the AFI system, including its search and aggregation capabilities, AFI was developed in coordination with the Privacy Office to minimize privacy risks. The Privacy Office also required that AFI undergo a PCR within 12 months of the system's operational deployment to assess compliance with existing compliance documentation, and to ensure the privacy protections in the PIA were followed. The first PCR on the AFI system was published on December 19, 2014, which reviewed AFI from August 2013 to May 2014, and resulted in 16 recommendations to enhance AFI privacy protections commensurate with its use. The 2014 PCR also noted that the Privacy Office would conduct a follow-up PCR twelve months from publication to assess the status of those recommendations.

On January 20, 2016, the Privacy Office launched its second PCR of AFI by developing and administering a questionnaire to the AFI program that covered operations from May 2014 to March 2016. The Privacy Office 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.

[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.

Due to the novel technologies and heightened privacy risks involved with the collection of biometrics, particularly with untested biometric modalities, the PIA for this test required the Privacy Office to conduct a PCR at the conclusion of the test. The PCR evaluated how the information collected during the test was used, retained, and destroyed. In keeping with the test goals of providing an operational feasibility assessment for potential future deployment, the resulting PCR's recommendations were intended to provide CBP with best practices and an initial privacy compliance framework for potential future deployments of biometric collection technologies and processes.

The Privacy Office found that CBP managed this test with privacy-protective objectives and with sensitivity to privacy and data aggregation risks, and the Privacy Office recommended that CBP consider the 10 best practices for any future biometric exit tests to further improve its ability to demonstrate compliance with privacy requirements.

Nationwide Suspicious Activity Reporting (SAR) Initiative, April 21, 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).

The November 2010 DHS ISE-SAR Initiative PIA and subsequent May 2015 update identified and assessed the privacy risks associated with DHS Components' participation in the NSI. One such potential risk identified in the 2010 PIA notes that adverse actions may potentially be taken against individuals based on inaccurate or incomplete information available in the NSI SDR. To reduce this risk, the 2010 PIA required PRIV to initiate a PCR within nine months of any new Component joining the NSI as an authorized participant, in order to ensure the new participant's adherence with the PIA and other privacy compliance documentation.

An initial PCR, completed in October 2012, resulted in five recommendations crafted to help ensure that privacy, civil rights, and civil liberties are protected when DHS Components participate in the NSI. These recommendations addressed the self-auditing of ISE-SAR

submissions, communication with the DHS Suspicious Activity Reporting Initiative Management Group, and both initial and refresher training regimens. The 2012 PCR offered up the Privacy Office's assistance in developing a self-audit structure, and noted that we would evaluate the need to conduct additional reviews of ISE-SARs to include Components whose submissions were not reviewed in 2012.

While no additional Components have joined the NSI as authorized participants since the 2010 PIA's publication, and although we did not complete follow-up actions mentioned in the 2012 memo, we did launch a follow-up to the 2012 PCR in October 2015 to assess whether Components had implemented the five recommendations from the 2012 PCR. We initiated this effort to determine whether current privacy protections in various DHS NSI areas, including auditing, reporting, training, and vetting, are sufficient, and to identify and potentially recommend further suggestions for any outstanding privacy issues associated with DHS Components' NSI participation.

In accordance with *DHS Privacy Policy Instruction 047-01-004*, we worked collaboratively with all ISE-SAR-submitting DHS Component NSI representatives and privacy offices, as well as the DHS NSI Program Management Office to promote privacy compliance and ensure privacy oversight. To finalize the PCR, we met individually with each Component to discuss the impetus for the PCR, its methodology, how its conclusions were reached, and what each specific privacy office could do to improve its Component's compliance with both NSI and privacy requirements. To follow up, Components will provide us with self-audit reports, and we reserve the right to review future ISE-SAR submissions to ensure compliance.

[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 launched a PCR based on the OIG recommendation, focusing on USSS privacy compliance on December 2, 2016.

The DHS Privacy Office recognizes USSS Privacy Office staffing shortages and significant changes in information technology systems that were underway during our review. We also recognize the resources needed to implement the OIG's recommendations to improve the USSS privacy posture.

USSS senior leadership was presented with the findings in our report. This PCR 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 USSS Privacy Office was tasked with providing a written report and supporting documentation on the implementation status of all recommendations by July 2018.

[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 biometrics information, PIAs for CPMS and NASS in 2015 required the DHS Privacy Office to conduct a PCR. During the course of this PCR, the DHS Privacy Office found USCIS to be in compliance with privacy requirements of federal privacy laws, DHS and Component privacy regulations and policies, and explicit assurances made by USCIS in existing privacy compliance documentation. We identified six recommendations designed to improve USCIS privacy compliance, and to incorporate best practices for other USCIS and DHS programs and systems.

PCRs With Ongoing Oversight

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

We conducted a PCR of the Office of the Chief Human Capital Officer (CHCO) in 2015 based on *DHS Privacy Policy Guidance Memorandum 2008-01*, which included 25 recommendations to improve the culture of privacy at CHCO. 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, The Privacy Office has met numerous times with the Chief Human Capital Officer and CHCO staff to encourage implementation of the recommendations, focusing on how CHCO will make sustainable plans and actions to perpetrate a culture change. CHCO submitted implementation status reports in 2016 and 2017 in compliance with the 2015 PCR biannual self-audit requirement.

The Privacy Office continues to seek more robust privacy practices and greater privacy awareness among CHCO personnel especially given their day-to-day work with PII.

[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 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.

PCRs Launched

- The Privacy Office launched a PCR of the DHS Countering Violent Extremism Grant Program (CVEGP) on January 18, 2017 to determine the degree of compliance with the [Office for Community Partnerships \(OCP\) CVEGP PIA](#) and [Privacy Policy Guidance Memoranda 2008-01/Privacy Policy Directive 140-06](#). This review is currently still in the due diligence stage. A final product has not yet been determined.
- On September 1, 2016, DHS issued an update to the PIA for the Electronic System for Travel Authorization (ESTA) in order to provide notice to the public, and assess the privacy risks associated with CBP's use of social media identifiers in the vetting of ESTA applications. On May 17, 2017, the Privacy Office launched a PCR to review the novel privacy risks surrounding the collection and operational use of social media information in relation to the ESTA application. We expect to finalize a public report in November 2017.

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).²¹ The CPO serves as the Chairperson of the DHS Data Integrity Board, and members include the Inspector General, the Officer for Civil Rights and Civil Liberties, the Office of the Chief Information Officer, and representatives of Components that currently have an active CMA in place.²²

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 DHS Data Integrity Board. CMAs are required when there is a comparison of two or more automated systems of records for the purpose of verifying the eligibility for cash or in-kind federal benefits.²³

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 recertified 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 DHS Data Integrity Board seeks to expose fraud and waste while ensuring that computer matching does not result in misuse or abuse of personally sensitive information (the latter concern prompted Congress to pass the Computer Matching and Privacy Protection Act). The DHS Data Integrity Board reviews CMA activity annually in December and submits an annual report to the Office of Management and Budget in June (the DHS Computer Matching Activity Report).

In the [DHS 2016 Computer Matching Activity Report](#), the DHS Data Integrity Board submitted a favorable cost benefit analysis for the overall program and reported the establishment of a new CMA between the Federal Emergency Management Agency and the United States Department of Housing and Urban Development (instituted in October 2016). The DHS Data Integrity Board was proud to approve this new disaster relief agreement to assist those in need of emergency housing. This CMA helped 2016 flood survivors and 2017 hurricane survivors receive benefits faster and more efficiently.

DHS is now partnered in [11 CMAs](#). Each CMA benefits the public by ensuring funding is not duplicated or erroneous, and protects the personally sensitive information of vulnerable

²¹ 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).

²² 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).

²³ 5 U.S.C. § 552a(o).

populations such as: needy families, small business owners, student loan recipients, and flood/natural disaster victims.

FOIA Compliance

FOIA requests:²⁴ DHS continues to receive the largest annual number of FOIA requests of any federal department or agency, receiving almost 40 percent of all requests within the Federal Government. In FY 2016, DHS received 325,780 FOIA requests and processed 310,549, the largest amount of requests received by an agency in one fiscal year.²⁵ This is a 16 percent increase from the previous fiscal year, which reflects a continued interest in current events, the DHS missions, and the activities of DHS Components.



The majority of FOIA requests were addressed to USCIS from individuals seeking immigration-related records. CBP, ICE, and the Office of Biometric Identity Management (OBIM) also received a large share of the requests. These Components combined received approximately 97 percent of all DHS FOIA requests in FY 2016.

FOIA backlog: The increased demand for immigration records directly affected the Department's backlog, which increased from 35,374 in FY 2015 to 46,788 in FY 2016. More than 76 percent of the Department's backlog resides with USCIS.

The growth in the backlog by itself does not explain the state of the FOIA program. Although the Department's backlog increased, four Components made significant strides in processing a record number of requests:

- CBP decreased its backlog by 87 percent despite receiving 28 percent more requests in FY 2016.
- NPPD decreased its backlog by 19 percent despite receiving 42 percent more requests in FY 2016.
- TSA decreased its backlog by 21 percent, responding to more than 67 percent more requests in FY 2016.
- ICE maintained a backlog of under 500 requests despite receiving 63,385 requests (a 42 percent increase) in FY 2016.

Reducing the backlog remained one of the Privacy Office's top priorities this year. The Privacy Office partnered with NPPD/OBIM leadership to execute an aggressive 40-day Backlog Reduction Plan. As a result of this partnership, the teams were able to reduce OBIM's backlog by 75 percent by the end of FY 2016, and reduce the Department's projected FY 2016 overall

²⁴ For efficiency, Departmental data reflects the reporting period used in the *Freedom of Information Act Annual Report*.

²⁵ The information regarding the Department's FOIA program is in the FY 2016 Annual FOIA Report available at <https://www.dhs.gov/foia-annual-reports> and will also be included in the 2017 Chief FOIA Officer Report, which is available at <https://www.dhs.gov/dhs-chief-foia-officer-reports>.

backlog by 26 percent. The teams processed more than 14,000 backlogged FOIA cases in 40 days.

Information Sharing and Intelligence Activities

Background

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: Privacy Office, Office of Intelligence and Analysis (I&A), Office of Policy (PLCY), OGC, and CRCL.

During the reporting period, the Privacy Office worked with DHS stakeholders and IC partners to approve 13 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 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 continued to support the deployment of the Texas Latent Interoperability Project. This program links Texas law enforcement agency investigative actions (through latent Texas crime scene prints) to DHS populations (i.e., law enforcement contacts, benefit applicants, and travel/access privilege applicants), to support Texas investigations and DHS mission needs.

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 outside the Federal Government. In addition, the Privacy Office checks 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 585 IIRs and FINTEL, 67 briefing packages, and 367 RFI (at all levels of classification). The Privacy Office also reviewed I&A's standing information requirements to ensure that DHS did not unintentionally 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. Much of the preparatory work for this change was completed during this reporting period; however, some technology issues remain to be resolved before this new approach can be fully implemented. The Privacy Office anticipates being able to make the transition during the next fiscal year. *Mission Number One: Prevent Terrorism and Enhance Security.*

Nationwide Suspicious Activity Reporting Initiative

This year, the Privacy Office continued training personnel responsible for analyzing and sharing terrorism-related Suspicious Activity Reports on the importance of adhering to the privacy protections contained in the ISE Functional Standard for Suspicious Activity Reporting and in the *DHS/ALL/PIA-032 - DHS Information Sharing Environment Suspicious Activity Reporting Initiative*. Analysts are trained, on average, every 90 days.

I&A, primarily through its State and Local Program Office in coordination with OPS, leads the DHS effort to implement the Nationwide Suspicious Activity Reporting Initiative (NSI). The NSI is a key aspect of the federal ISE that Congress created in the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA). The NSI is a collaborative effort by DHS, the Federal Bureau of Investigation (FBI), and state, local, tribal, and territorial law enforcement partners. It is designed to support the sharing of information through the ISE about suspicious activities. NSI shares “official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity [related to terrorism].”

Mission Number One: Prevent Terrorism and Enhance Security.

Privacy Incident and Complaint Handling

Privacy Incidents

The Privacy Office manages privacy incident response for the Department. Privacy Office staff work to ensure that all privacy incidents are properly reported, investigated, mitigated, and remediated as appropriate for each incident, in collaboration with the DHS Enterprise Security Operations Center (ESOC), Component Security Operations Centers (SOC), Component privacy officers and PPOCs, and DHS management.



The Privacy Office authored the [DHS Privacy Incident Handling Guidance](#) (PIHG), the foundation of DHS privacy incident response.

DHS defines a privacy incident²⁶ as, with regard to PII, the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII; or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which result in a reasonable risk of harm.

In response to OMB guidance issued in January 2017, [Memorandum M-17-12, Preparing for and Responding to a Breach of PII](#), we issued one new privacy policy and two completely revised privacy policy instructions this year:

1. New: *Privacy Incident Responsibilities and Breach Response Team*:²⁷
 - a. Establishes DHS policy, responsibilities, and requirements for responding to all incidents involving PII contained in DHS information; and
 - b. Establishes the requirement for the CPO to convene and lead a Breach Response Team, when a “major incident” involving PII has occurred,²⁸ or at the discretion of the CPO.

²⁶ DHS changed its long standing definition of privacy incident to comport with OMB’s definition of a **breach** in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of PII* (Jan. 3, 2017), but added the final sentence to address suspected and confirmed incidents. We kept the term “privacy incident” to be consistent with other DHS incident types.

²⁷ To be published on DHS.gov in November 2017.

²⁸ 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-17-015 and

-
2. Revised: [*Privacy Incident Handling Guidance*](#) (PIHG) addresses all types of privacy incidents (paper, electronic, web-based, or physical occurrence) and includes guidance for reporting and handling privacy incidents, as well as checklists for handling all stages of minor and major privacy incident.
 3. Revised: *Handbook for Safeguarding Sensitive PII*²⁹ 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.*



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, 776 confirmed privacy incidents were reported to the DHS SOC, an increase of 11 percent from the last reporting period. Figure 6 shows the total number of both suspected and confirmed privacy incidents, broken down by Component.

subsequent OMB guidance. 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.

²⁹ To be published on DHS.gov in November 2017.

Component	Suspected Incidents	Confirmed Incidents
CBP	12	11
DHSHQ	17	4
FEMA	14	14
FLETC	3	1
ICE	52	48
Master ³⁰	270	327
NPPD	12	11
OBIM	4	2
OIG	1	1
TSA	9	5
USCG ³¹	94	100
USCIS	331	252
S&T	1	0
USSS	3	0
Total	823	776

Figure 6: Total number of suspected and confirmed privacy incidents by DHS Component for the time period July 1, 2016 – June 30, 2017

During the reporting period, the Privacy Office continued its efforts to reduce privacy incidents and ensure proper incident handling procedures by:

- Analyzing incident trends and trouble shooting incident causes to promote prevention efforts.
- Designing an internal privacy awareness communications plan to encourage all staff to report privacy incidents immediately, and convey best practices to prevent an incident.
- Participating in the Federal Privacy Council’s Federal Breach Response and Identity Theft Subcommittee to share best practices with other federal agencies.

³⁰ A Master Incident occurs when multiple Components are involved in a single privacy incident.

³¹ The discrepancy for USCG and Master Incidents is due to suspected incidents reported before July 1, 2016 that were escalated to confirmed incidents during this reporting period.

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 2007,³² 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.³³ U.S. citizens, Lawful Permanent Residents, visitors to the United States, and aliens may submit privacy complaints to the Department.³⁴ 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 general 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), we 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.³⁵ See the section below on Non-Privacy Act Redress Programs for more details.

³² 42 U.S.C. § 2000ee-1(f).

³³ These semi-annual reports may be found here: <https://www.dhs.gov/publication/dhs-section-803-reports-congress/>.

³⁴ 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 new 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.

³⁵ As required by PRIV's Memorandum of Understanding with OIG, established due to 222 of the Homeland Security Act, we receive monthly reports of any privacy-related complaints received in that Office and OIG's disposition of those complaints. OIG follows a similar process of referring complaints to relevant Components or to us, as appropriate. As a result of Privacy Policy and Oversight's working relationship with OIG, we review all draft OIG reports for PRIV.

Between April 1, 2016 and March 31, 2017, the Department received 2,061 privacy complaints and closed 2,097. Figure 6 shows the categories and disposition of privacy complaints the Department received.

Type and Disposition of Privacy Complaints Received³⁶				
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	0	3	0	3
Redress	332	331	1	0
Operational	1,727	1,761	25	1
Referred	2	2	0	0
Total	2,061	2,097	26	4

*Figure 6: Privacy Complaints Received by DHS
April 1, 2016 – March 31, 2017*

³⁶ 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, to request amendment of his or her own records.³⁷ 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 2016 – June 2017				
Component	Received	Granted	Denied	Pending
FEMA	1		1	
ICE	10	2	7	1
Coast Guard	1		1	
USCIS	22	2	4	16
USSS	1			1
TOTALS	35	4	13	18

³⁷ 5 U.S.C. § 552a(d)(2).

Non-Privacy Act Redress Programs

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

- **DHS Traveller Redress Inquiry Program (DHS TRIP).**³⁸ DHS TRIP offers redress services to the public by providing a centralized processing point for individual travellers 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 15,431 requests for redress, with an average response time (date case opened to date case closed) of approximately 37 days.
 - The CPO is a member of the DHS TRIP Advisory Board, and the Privacy Office is an active DHS TRIP practitioner. Redress inquiries alleging non-compliance with DHS privacy policy are reviewed by the Privacy Office, and they are either referred to the relevant Component, or are handled by the Privacy Office, as appropriate.
- **NPPD/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.
 - NPPD/OBIM responded to 148 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 feel that 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 5,525 appeals and denied 431.
 - Additionally, OIA granted 2,949 waivers and denied 199.

³⁸ <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.

Workforce

At the close of the reporting period, the Privacy Office had a total staff of 46: 33 employees, four detailees, and nine contractors, which include the following back-filled positions:

- Senior Director of Privacy Policy and Oversight
- Senior Director for Information Sharing, Security, and Safeguarding
- Senior Advisor to the Chief Privacy Officer
- Senior Privacy Analyst
- Privacy Analyst, Presidential Management Fellow
- FOIA analyst

Recruitment actions are underway to fill these vacant positions:

- Senior Director, FOIA Operations and Management
- Senior Director, Privacy Compliance
- Senior Privacy Analyst
- Freedom of Information Act Analysts
- Administrative Specialist

Budget

In FY 2016, our full year actual budget³⁹ was \$8,184,423. In FY 2017, our enacted level was \$7,851,000, \$333,423 below our FY 2016 actual budget. We were able to operate at this reduced funding level primarily through attrition. In addition, we continued to carry out the duties required in our operating authority through the following innovations and cost saving efforts:

1. Leveraged intra-agency agreements with 14 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 \$492,504 in reimbursable funding, which allowed us to direct more resources toward our privacy and FOIA support services contracts; and
3. Conducted a review of our IT billing, data management and support requirements, resulting in an annual cost savings of \$245,000 for the Department.

Employee Engagement

The Staff Advisory Council (SAC), established by the CPO in 2014, continues to play a significant role in strengthening employee morale, encouraging collaborative initiatives, promoting a healthy work-life balance, and fostering communication between management and staff. The SAC was formally chartered to be an enduring source of support for Privacy Office staff, and a useful advisory body for the CPO. The SAC has supported the CPO in facilitating openness and transparency, and fostering a work environment that encourages teamwork and a commitment to excellence. Based on SAC recommendations from focus groups conducted with the staff, the Privacy Office has implemented many new and innovative initiatives, and incorporated diversified approaches that have been beneficial and advantageous to the entire office. Privacy Office management is dedicated to implementing programs, policies, and practices that result in positive employee engagement in order to retain a resilient and motivated workforce.

³⁹ Actuals are based on the enacted or revised enacted (where applicable) budget, appropriated funding levels, or reimbursement funding from other government entities.

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. Numerous staff spoke at conferences sponsored by prominent national associations for privacy and disclosure professionals.

In addition, management is dedicated to mentoring students. To this end, the Privacy Office partnered with several colleges and universities throughout the year to provide opportunities for student internships within the Privacy Office.

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 privacy 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. During the current reporting period, The FEMA Privacy Office was reorganized under the newly established Information Management Division (IMD), which also includes the Records Management and Disclosure Branches. The FEMA Privacy Office was renamed the Privacy Branch (FEMA Privacy), but all operations, functions, and processes remain the same; 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

- Continued to respond to two privacy-related recommendations from the June 2016 DHS Office of the Inspector General (OIG) Management Advisory Report, “FEMA Continues to Experience Challenges in Protecting Personally Identifiable Information at Disaster Recovery Centers,” to ensure that: (1) all FEMA personnel at disaster relief sites complete mandatory privacy awareness training and are aware of their responsibilities to protect PII; and (2) FEMA conducts timely privacy compliance site assessments to ensure privacy protections are being implemented throughout FEMA disaster operations, to include disaster recovery centers. To comply with OIG’s recommendations, FEMA expanded its Privacy Point of Contact (PPOC) Council to appoint PPOCs for Disaster Operations. The PPOC for Disaster Operations serves as an extension of the FEMA Privacy Branch. This is accomplished through a partnership with the Office of the Chief Security Officer (OCSO) that integrates privacy functions into the existing disaster operations functional framework for the Security Cadre, who are deployed at every disaster. This will ensure that at least one PPOC is designated to every disaster to provide privacy training, disseminate privacy resource materials, and conduct privacy compliance site assessments at disaster worksites.

-
- 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.
 - Provided privacy awareness training and site assessments to FEMA Program Offices within the National Capital Region (NCR), as well as FEMA Regional Offices.
 - Represented privacy interests on the Grants Modernization IPT as it relates to the Agency-wide initiative to consolidate and modernize information technology systems that administer FEMA grants programs.
 - Represented privacy interests on the Information Governance Working Group (IGWG) as it relates to privacy topics surrounding the use of FEMA SharePoint and collaboration sites. The mission of the working group is to ensure that proper privacy notifications are in place to remind employees how to appropriately protect PII on the SharePoint sites.
 - Continued to report moderate to high-level privacy incidents to senior executives within the agency. This process establishes a level of visibility into privacy incident response and mitigation, and keeps senior leadership apprised of high-level incidents.
 - 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.
 - 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: 86 percent for PIAs and 97 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:

The Federal Insurance and Mitigation Administration (FIMA) National Flood Insurance Program (NFIP) completed the *DHS/FEMA/PIA – 011a National Flood Insurance Program Information Technology Systems (NFIP ITS) PIA* for the FEMA NFIP Reinsurance Program (NRP). The NRP transfers some of the monetary risk of flood insurance from the Federal Government to private capital firms or reinsurance companies. This process will reduce tax dollars used to fund flood insurance claims that exceed premiums paid into the NFIP by NFIP policy holders. The PIA allows FIMA to use flood insurance policy holders’ information to create risk models that capital firms and reinsurance companies need to access their stakeholder’s vulnerabilities by accepting NFIP flood insurance risk and initiate contracts or agreements with FIMA.

Computer Matching Agreements:

- Executed a CMA between FEMA and the U.S. Department of Housing and Urban Development to enable record matching to help transition presidentially-declared disaster survivors from temporary housing to long-term housing more efficiently and prevent duplication of benefits.
- Executed a CMA renewal between FEMA and the Small Business Administration (SBA) to enable record matching to prevent duplication of benefits during a presidentially-declared disaster.

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 enables NPPD to execute its mission while ensuring the preservation of individual privacy across all five of DHS’s mission goals: Preventing Terrorism and Enhancing Security, Securing and Managing Our Borders, Enforcing and Administering Our Immigration Laws, Safeguarding and Securing Cyberspace, and Ensuring Resilience to Disasters.

During this reporting period, the NPPD Office of Privacy increased its ability to protect privacy by filling vacant privacy positions to support critical mission operations. For example, the NPPD Office of Privacy now has a dedicated privacy analyst that supports the Federal Protective Service (FPS). Another new privacy analyst ensures that the Office of Cybersecurity and Communications (CS&C) programs address privacy equities.

The NPPD Office of Privacy supported a number of significant activities to promote and protect privacy while supporting critical mission operations at NPPD including FPS, OBIM, Office of Infrastructure Protection (IP), Office of Cyber and Infrastructure Analysis (OCIA), and CS&C.

Privacy Policy and Compliance Leadership

- At the request of the former Acting CPO, the NPPD Office of Privacy and National Protection and Programs Law Division (NPPLD) performed a privacy analysis and a legal analysis, respectively, of CS&C’s Cybersecurity Information Handling Guidelines as required by the Federal Cybersecurity Enhancement Act.

-
- Conducted two Privacy Oversight Reviews⁴¹ of NPPD’s cybersecurity programs focusing on CS&C’s EINSTEIN and Cyber Information Sharing and Collaboration Program.
 - In addition to Privacy Oversight Reviews, the NPPD Office of Privacy continues to evaluate the effectiveness of CS&C’s Automated Indicator Sharing initiative “privacy scrub,” and performs regular product reviews of OCIA analytical reports.
 - Participated in the DHS Privacy Office assessments of NPPD activities under Executive Order 13636 and Executive Order 13691.
 - Conducted 300 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 made contributions to the federal privacy enterprise through the following activities:

- NPPD’s Senior Privacy Officer served as a co-author of the privacy requirements and considerations included in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63, Digital Identity Guidelines, published on June 22, 2017.
- NPPD’s Senior Privacy Officer also made contributions to the Federal Privacy Council by teaching two sessions of the newly-established “Privacy Boot Camp” on IT security for privacy professionals, and by co-chairing the Federal Privacy Council’s Digital Authentication Task Force, which provided input into the newly published NIST SP 800-63, Digital Identity Guidelines.
- The NPPD Office of Privacy staff are also actively engaged with the Federal Privacy Council by attending or participating in its training events and working groups.

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 compliance documents published during the reporting period:

- Training and Academy Management System – NPPD’s Federal Protective Service (FPS) acquired a robust automated training system to provide FPS with tracking, monitoring, and verification of training for federal law enforcement and security personnel, and to empower these personnel with the skills and knowledge necessary for effective and safe enforcement of the law.

⁴¹ In response to a 2011 Privacy Compliance Review recommendation by DHS PRIV 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 the privacy compliance of the programs with existing documentation (such as standard operating procedures and work aides) and their operational products and activities, and to provide recommendations to strengthen program oversight, privacy preserving information sharing, and to ensure the programs are in full compliance with data retention and training policies.

-
- Chemical Facility Anti-Terrorism Standards Personnel Surety Program - 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.

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 adequately 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

- Expanded its staff from a single Privacy Officer to include a Deputy Privacy Officer and a Privacy Assistant, allowing the Office to delegate responsibilities for the various privacy-related duties and devote considerably more time and effort to each of them.
- Partnered with the DHS Privacy Office on the National SAR Initiative (NSI) privacy compliance review. *See Chapter 3 for more information on this PCR.*
- Participated as a key member in a number of DHS-wide groups and committees, including the Social Media Task Force, the DARC, and the Data Framework Working Group.
- Currently revising I&A's training regime to develop more extensive privacy training for new employees during orientation, role-based training for employees and contractors who handle PII, and an outreach and awareness campaign centered around protecting PII.
- Partners with the DHS Privacy Office 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.

Privacy Compliance

- I&A, as an element of the IC, is exempt from FISMA reporting requirements.
- Partnered with the CIO to ensure that privacy documentation is in place before any new IT investment is approved.

Science and Technology Directorate (S&T)



S&T manages science and technology research to protect the homeland, from development through transition, for DHS Components and first responders. S&T's mission is to strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the homeland security enterprise. Since 2015, S&T, via the Cyber Security Division, has had a privacy research program supporting DHS Privacy Office goals.

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

Privacy Policy Leadership

Over the past year, S&T Privacy helped build and maintain privacy best practices for research, development, testing, and evaluation activities, including biometric entry and exit projects, social media vetting tools analyses, and unmanned aircraft projects. The privacy best practices they embed into all of their test systems bring potentially invasive technologies into compliance with federal privacy and civil liberties statutes and protections, and also support DHS mission goals to secure our borders, prevent terrorism, and enforce and administer immigration laws.

For example, in response to airport processing delays encountered by passengers entering the United States, S&T is working with CBP to conduct several test and evaluation projects to determine where the bottlenecks are occurring. A number of different technologies ranging from enhanced self-check-in kiosks to unique tokens in the form of Quick Response Codes will be tested and evaluated. The results will help CBP determine which technologies can enable the processing of more passengers within existing CBP staff levels.

Privacy Compliance

FISMA scores: 100 percent for both PIAs and SORNs.

All S&T 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.

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 airport security screening efforts at more than 450 airports, but is also responsible for the security of other modes of transportation, including highways, maritime ports, railways, mass transit, and pipelines.

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,
 - 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,
 - ingesting TSA data into the DHS Data Framework for the full-range of DHS missions, including law enforcement, intelligence, and immigration, and
 - ingesting TSA data into OBIM systems.
- As a member of the TSA Security Threat Assessment Board, provided a privacy and civil liberties review of proposed actions against transportation sector worker credentials, and 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 12 programs to ensure that PIAs adequately represented the program.
- Reviewed more than 310 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 (USCIS Privacy) works diligently to promote a culture of privacy across USCIS, to sustain privacy protections in USCIS programs, directorates, and initiatives, and to enhance the privacy awareness of all personnel. It pursues this goal by developing policies, conducting privacy training and awareness activities to help reduce privacy incidents, and participating in privacy-related working groups.

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

Privacy Policy Leadership

- Established the Program/Directorate Leads Branch to provide privacy oversight and compliance to major program offices and directorates, and to manage the information sharing program within USCIS.
 - *The Program/ Directorate Leads Team:* Established this team to monitor and review multiple Agile development processes to ensure privacy is considered throughout this fast-paced and often changing environment. In the Agile environment, the team provides periodic briefings of the direction in which processes are headed, input into user stories (business requirements), and continuous governance to promote privacy. Checkpoints for privacy have been built into these processes to quickly identify privacy issues and remedy them.
 - *The Information Sharing Program:* Established an information sharing program to provide ways to facilitate information sharing requirements between internal and external stakeholders (federal, state, local, and international organizations).

-
- **Hired a new Privacy Training Officer:** The new training officer will ensure that USCIS is in compliance with all federal privacy training requirements. The officer will also develop and deliver a variety of privacy and transparency-related training to USCIS personnel and key stakeholders. The training officer has standardized and centralized all of the instructor-led privacy trainings. In addition, the training officer is conducting a major update to the current mandatory online privacy awareness training that is specific to USCIS, looking at ways to incorporate privacy training into other programs' and directorates' training programs, and finding creative ways to provide training such as webinars, video conference, etc.
 - **Provided guidance to USCIS' programs and directorates to ensure the implementation of operational use of social media protects the privacy, civil rights, and civil liberties of those who will be subject to social media searches.** As USCIS prepares to effectively operationalize the use of social media in response to evolving threats and in accordance with directives from the White House, DHS, or USCIS operations, it is important for USCIS to broaden its operational testing and general understanding of how to best leverage publicly available information located on social media sources. This information has potential to safeguard our national security, enhance public safety, combat benefit or relief fraud, investigate allegations related to employee misconduct, enrich research-related products, and ensure that benefits or relief are only granted to those who are statutorily eligible or meet policy guideline qualifications.

Privacy Compliance

FISMA scores: 96 percent for PIAs and 100 percent for SORNs.

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.

- Participated in working groups to implement Section 14 of Executive Order 13768, *Enhancing Public Safety in the Interior of the United States*. See Chapter 1 for more information.
- Conducted 12 privacy security compliance reviews with HQ program offices. These reviews are designed 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.

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 Coast Guard employs its broad authorities, expansive network of interagency, military, 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 Assistant Commandant for Intelligence (CG-2) to outline USCG's mission, roles, and responsibilities for inclusion in CBP's Analytical Framework for Intelligence PIA.
- Developed a privacy dashboard that provides metrics to senior leadership on USCG outstanding privacy incidents and compliance documentation.
- Coordinated response to several major privacy incidents impacting over 21,000 USCG personnel. Researched each incident extensively, engaged responsible commands to determine root cause, and provided viable recommendations to thwart future incidents. Ensured all impacted parties were provided resources to safeguard their identity and financial interests.
- Teamed with USCG Health Insurance Portability and Accountability Act (HIPAA) representatives and issued a notice prohibiting personal electronic devices in patient treatment areas.

-
- Added USCG Privacy as the final reviewer for all ALCOAST⁴² messages disseminated to field commands.
 - Provided a Weekly Privacy Incident Report to USCG Chief Information Officer (CIO) detailing open privacy incidents.
 - Disseminated guidelines for safeguarding PII and informational posters to USCG Information System Security Officers (ISSO) to promote best practices within the agency.
 - Collaborated with USCG Web Portals Management Branch to strengthen SharePoint restrictions by incorporating banners that indicate whether sensitive PII is allowed or not allowed on a Human Resource SharePoint website containing sensitive PII.
 - Established the USCG Privacy Officer as a permanent voting member of the CG Enterprise Architecture Board, which conducts reviews of emerging IT initiatives within the organization.
 - Responded to the Department of Defense PII Repository Hardening data call, and identified a privacy system in the USCG CIO's inventory.

Privacy Compliance

- FISMA scores: 97 percent for PIAs and 100 percent for SORNs.
- Reviewed directives, forms, and information collection as a part of the clearance process, which resulted in additional Privacy Act statements, submission of compliance documentation, etc., to ensure adherence to current federal privacy mandates.

The DHS Privacy Office assisted USCG Privacy in the development and publication of the Direct Access PIA. Direct Access is the primary system for human resource lifecycle and payroll support for over 100,000 active duty, reserve, and retired personnel at several agencies: DHS, Department of Health and Human Services, United States Public Health Service, Department of Commerce, and the National Oceanic and Atmospheric Administration.

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.

⁴² ALCOAST Messages: General administrative announcements used for award solicitations, education opportunities, half-masting, or other generic events.

U.S. Customs and Border Protection (CBP)



CBP guards the Nation's borders while fostering economic security through lawful international trade and travel. CBP's unique role at the border provides it with access to a broad array of data concerning people and merchandise arriving into and departing from the United States. CBP officials use and share the data for a variety of border security, trade compliance, and law enforcement purposes.

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

Privacy Policy Leadership

- Hired a new CBP Privacy Officer and six new staff members to work on privacy compliance, policy, and oversight functions. Transitioned the Privacy Office to a portfolio-based approach, with designated analysts providing privacy guidance and expertise to CBP offices.
- Published a CBP Privacy Strategic Plan and corresponding implementation plan, with cascading goals incorporated into leadership and staff performance plans.
- Formed staff-led working groups to revamp privacy communication and training initiatives, develop strategies for information governance and mobile application oversight, and revive the privacy liaison program.
- Developed the Border Searches of Electronic Devices Working Group to review current practices related to CBP searches of electronic devices, including mobile phones, at the border; work with the CBP Office of Chief Counsel and Office of Field Operations to develop a new directive on border searches of electronic devices; and re-assess the privacy impacts of these practices in preparation for an updated PIA.
- 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 draft CBP's implementation policy regarding the release of information to the media about non-U.S. citizen/non-Lawful Permanent Residents.

Privacy Compliance

- FISMA scores: 92 percent for PIAs and 100 percent for SORNs, the highest scores ever achieved by CBP Privacy.
- Advanced the privacy compliance program by requiring PTAs for 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.
- Worked with the DHS Privacy Office to complete PCRs for the Analytical Framework for Intelligence (AFI) and the Southwest Border Pedestrian Exit Field Test. The AFI PCR, a follow-up to a PCR conducted in 2014, found that CBP continued to operate and manage AFI with privacy-protective objectives and with sensitivity to privacy and data aggregation risks. In addition, DHS Privacy found that CBP complied with its privacy plan for the Southwest Border Pedestrian Exit Field Test, and issued a report containing only best practices for future tests, rather than recommendations requiring corrective action. See page 43 for more details on these PCRs.

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:

Traveler Verification Service (TVS): CBP Privacy worked closely with the CBP Entry and Exit Transformation Office to successfully launch TVS, providing recommendations for privacy enhancements and publishing a number of compliance documents, in close coordination with the DHS Privacy Office. U.S. airports, unlike many other airports around the world, are not designed with controls to verify identities of passengers departing the United States. Rebuilding U.S. airports would be costly and unnecessary if the goal is to confirm a traveler's identity. Instead, biometrics can be used to verify departing travelers' identities and meet CBP's congressional mandate. CBP's goal is to expedite movement of lawful travelers while enhancing national security, and using biometrics to protect a traveler against identity theft.

TVS uses CBP's biographic Advance Passenger Information System (APIS) manifest data and existing photographs of all travelers boarding international flights to confirm the identities of travelers, create exit records, and biometrically confirm the exit of in-scope non-U.S. citizens. The sensitivity of biometric collection at new locations (airports) involving new populations (all travelers) has generated a great deal of public interest and questions from privacy advocacy groups. To clarify misconceptions and provide a forum for discussion, CBP Privacy and the CPO met with privacy advocates to explain DHS's biometric exit initiatives, and address their questions and concerns.

- Published two new SORNs for Border Patrol enforcement records and CBP intelligence records to provide clearer notice and access procedures for major CBP information collections.
- Collaborated with the CBP Office of Information and Technology to develop a privacy oversight and compliance strategy for systems moving from 3-year authorization cycles into ongoing authorization.

United States Immigration and Customs Enforcement (ICE)



ICE is the principal investigative arm of DHS and the second largest investigative agency in the Federal Government. ICE promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

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

Privacy Policy Leadership

ICE established the Victims of Immigration Crime Engagement (VOICE) Office in April 2016, pursuant to Executive Order 13768, to provide assistance to victims of crimes committed by aliens. Specifically, the VOICE Office provides information to victims (when legally appropriate) in an effort to bring them some degree of comfort, and refers victims to other resources, such as victim service organizations. ICE Privacy worked closely with VOICE leadership and other ICE stakeholders to launch the office, and developed policy and procedural guidance on disclosures for the VOICE office. This guidance established a tiered review and approval process for disclosures to victims that accounts for legal, policy, and operational considerations. It permits VOICE to respond in an efficient manner to victims by empowering VOICE leadership to approve the release of specific types of information, and opening a channel to coordinate with ICE Privacy when additional releases of privacy sensitive information may be warranted.

Privacy Compliance

- FISMA scores: 95 percent for PIAs and 100 percent for SORNs.
- Responded to 10 Privacy Act amendment requests and one privacy complaint.
- Reviewed over 224 proposed procurements to ensure the inclusion of appropriate privacy protections in contract language.
- Resolved an estimated 91 privacy incidents, taking various steps to mitigate any damages from the incidents and prevent future incidents.

-
- Provided advice and oversight during the development of 12 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:

- **PIA on Victim Information and Notification Exchange (VINE):** VINE automatically notifies certain individuals about changes to a particular alien’s custodial status with ICE. These particular aliens include those who have been charged with or convicted of a crime, so long as a crime victim or victim advocate has registered with DHS-VINE to be notified upon change to the alien’s custodial status with ICE. Individuals eligible to receive custody status notifications include victims and witnesses associated with aliens charged with or convicted of a crime (at the federal or state level), as well as “victim advocates.”
- **SORN on Homeland Security Investigations Forensic Laboratory System of Records (HIS-FL):** This system of records allows ICE to collect and maintain records by the HSI-FL, a crime laboratory specializing in scientific authentication, forensic examination, research, analysis, and training related to travel and identity documents, latent and patent finger and palm prints, and audio and video files. These activities support law enforcement investigations and actions by DHS and other agencies.
- **SORN on the Criminal Arrest Records and Immigration Enforcement Records System of Records:** This SORN updates, renames, and reissues a current DHS system of records titled, *DHS/ICE-011 Immigration and Enforcement Operational Records (ENFORCE)*, system of records. ICE collects, uses, and maintains ENFORCE to support the identification, apprehension, and removal of individuals unlawfully entering or present in the United States in violation of the Immigration and Nationality Act, including fugitive aliens. ICE also uses ENFORCE to support the identification and arrest of individuals (both citizens and non-citizens) who commit violations of federal criminal laws enforced by DHS.

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 DHS Privacy Office worked collaboratively with the Secret Service Privacy Office to improve its privacy operations, develop necessary compliance documentation, and enhance privacy-protective practices among USSS personnel and programs. Over the past year, the DHS Privacy Office has assisted USSS with the drafting and review of a number of Privacy Impact Assessments associated with privacy sensitive systems that fall within its FISMA inventory. Additionally, the DHS Privacy Office conducted a PCR that assessed the current state of the USSS Privacy Office. The PCR identified a number of ways in which the Secret Service could strengthen its Privacy Office operations, as well as cultivate a culture of privacy within the agency. See Chapter 3 for more information on the USSS PCR.

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

Privacy Policy Leadership

- 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.
- Reviewed and conducted privacy risk assessments of new and updated USSS procurements of IT systems to ensure compliance with DHS guidance Class Deviation 15-01 from the

Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information. These reviews assessed the need to strengthen the security of contractor IT systems and define contractor responsibilities when responding to a privacy or sensitive information incident.

- Reviewed IT waiver and/or exception requests submitted by the OCIO for systems processing PII to assess privacy implications.
- 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: 92 percent for PIAs and 100 percent for SORNs.
- Reviewed and drafted Privacy Act statements for new and existing USSS forms.

The DHS Privacy Office assisted Secret Service Privacy in developing a PIA for the USSS Counter Surveillance Division's (CSD) 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. This Proof of Concept helped to determine the potential future use of tethered sUAS in supporting the USSS protective mission. The PIA evaluates the privacy risks associated with tethered sUAS's surveillance and image capturing capabilities.

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;⁴³
- (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.

⁴³ 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, and 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 Compliance Team for review and approval. The CPO conducts a final review before signing. 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.⁴⁴ 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.⁴⁵

⁴⁴ 5 U.S.C. § 552a(e)(4).

⁴⁵ 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, 2016 – June 30, 2017		
Component	Name of System	Date Published
CBP	DHS/CBP/PIA-021 TECS System	08/15/2016
CBP	DHS/CBP/PIA-002(c) - Global Enrollment System	11/02/2016
CBP	DHS/CBP/PIA-038 Cornerstone	02/27/2017
CBP	DHS/CBP/PIA-035 Complaint Management System (CMS)	09/16/2016
CBP	DHS/CBP/PIA-010(a) - Analytical Framework for Intelligence (AFI)	09/02/2016
CBP	DHS/CBP/PIA-025 Radiation Detection Systems	07/11/2016
CBP	DHS/CBP/PIA-032 Human Resources Business Engine (HRBE)	07/26/2016
CBP	DHS/CBP/PIA-033 Electronic Visa Update System (EVUS)	09/12/2016
CBP	DHS/CBP/PIA-034 Enterprise Management Information System-Enterprise Data Warehouse (EMIS-EDW)	09/08/2016
CBP	DHS/CBP/PIA-007(c) Electronic System for Travel Authorization (ESTA)	09/15/2016
CBP	DHS/CBP/PIA-004(h) Beyond the Border Entry/Exit Program Phase III	08/15/2016
CBP	DHS/CBP/PIA-036 CBPTradePulse	10/05/2016
CBP	DHS/CBP/PIA-025(b) 1-to-1 Facial Comparison Project	10/25/2016
CBP	DHS/CBP/PIA-037 Pre-Arrival Readiness Evaluation (PARE)	11/21/2016
CBP	DHS/CBP/PIA-030 Departure Verification System	12/19/2016
CBP	DHS/CBP/PIA-039 CBP Situation Room	02/28/2017
CBP	DHS/CBP/PIA-006(e) Automated Targeting System	01/17/2017
CBP	DHS/CBP/PIA-024 Arrival Departure Information System (ADIS)	04/28/2017
CBP	DHS/CBP/PIA-040 Seized Assets and Case Tracking System (SEACATS)	04/11/2017
CBP	DHS/CBP/PIA-043 CBPnet	05/11/2017
CBP	DHS/CBP/PIA-042 Workbench 2.0	05/09/2017
CBP	DHS/CBP/PIA-041 Enterprise Geospatial Information Services (eGIS)	05/03/2017
CBP	DHS/CBP/PIA-030(b) Traveler Verification Service (TVS)	05/15/2017

Privacy Impact Assessments Published July 1, 2016 – June 30, 2017		
Component	Name of System	Date Published
CBP	DHS/CBP/PIA-006(e) ATS PIA Addendum for Retention of Data from Electronic Devices	05/01/2017
CBP	DHS/CBP/PIA-030(c) Traveler Verification Service (TVS): Partner Process	06/12/2017
DHS-Wide	DHS/ALL/PIA-055 DHS Intelligence Enterprise Data Analysis Tools	08/08/2016
DHS-Wide	DHS/ALL/PIA-058 DHS Access Lifecycle Management	01/25/2017
DHS-Wide	DHS/ALL/PIA-014 Personal Identity Verification/Identity Management System (PIV/IDMS)	05/09/2017
DHS-Wide	DHS/ALL/PIA-25(a) - Accessibility Compliance Management System (ACMS)	03/29/2017
DHS-Wide	DHS/ALL/PIA-013 Procurement Request Information System Management (PRISM)	04/24/2017
DHS-Wide	DHS/ALL/PIA-060 Application Authentication System	02/28/2017
DHS-Wide	DHS/ALL/PIA-044(a) Single Point of Service Request for Information Tool	03/23/2017
DHS-Wide	DHS/ALL/PIA-059 Employee Collaboration Tools	02/07/2017
DHS-Wide	DHS/ALL/PIA-014(e) Personal Identity Verification/Identity Management System (PIV/IDMS)	05/18/2017
DHS-Wide	DHS/ALL/PIA-038(c) Integrated Security Management System (ISMS)	06/26/2017
FEMA	DHS/FEMA/PIA-042 Emergency Operations Center Network (EOCNET)	12/19/2016
FEMA	DHS/FEMA/PIA-011(a) National Flood Insurance Program Information Technology System (NFIP ITS)	09/29/2016
FEMA	DHS/FEMA/PIA-045 Hazard Mitigation Planning and Flood Mapping Products and Services Support Systems	06/27/2017
FEMA	DHS/FEMA/PIA-043 Contact Center Capability Modernization Program (C3MP)	04/13/2017
FEMA	DHS/FEMA/PIA-044 National Fire Incident Reporting System (NFIRS)	06/14/2017
FLETC	DHS/FLETC/PIA-001 Enterprise Security System (ESS)	12/22/2016
ICE	DHS/ICE/PIA-001(b) Student and Exchange Visitor System Admissibility Indicator (SEVIS-AI)	07/21/2016
ICE	DHS/ICE/PIA-044 LeadTrac	08/03/2016

Privacy Impact Assessments Published July 1, 2016 – June 30, 2017		
Component	Name of System	Date Published
ICE	DHS/ICE/PIA-046 Laboratory Information Management System (LIMS)	12/21/2016
ICE	DHS/ICE/PIA-047 Victim Information and Notification Exchange (DHS-VINE)	01/10/2017
ICE	DHS/ICE/PIA-001(c) Student and Exchange Visitor Information System (SEVIS); Student and Exchange Visitor Program Automated Management System (SEVPAMS); and SEVP External Training Application (SETA)	06/23/2017
NPPD	DHS/NPPD/PIA-009(a) Chemical Facility Anti-Terrorism Standards (CFATS)	08/15/2016
NPPD	DHS/NPPD/PIA-024 FPS Training and Academy Management System	08/25/2016
NPPD	DHS/NPPD/PIA-030 Continuous Diagnostics and Mitigation	09/30/2016
NPPD	DHS/NPPD/PIA-018(c) Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program	05/11/2017
OPS	DHS/OPS/PIA-008 HSIN R3 User Accounts HSIN Exchange Flash Alerts	04/25/2017
S&T	DHS/S&T/PIA-031 Select Agent Inventory Plum Island Animal Disease Center	12/27/2016
TSA	DHS/TSA/PIA-011(a) Airmen Certificate Vetting Program	09/22/2016
TSA	DHS/TSA/PIA-004(c) Visitor Management System	01/11/2017
USCG	DHS/USCG/PIA-024 Direct Access	11/16/2016
USCG	DHS/USCG/PIA-002(d) Biometrics at Sea System (BASS)	12/07/2016
USCG	DHS/USCG/PIA-001(c) Homeport Internet Portal	06/19/2017
USCIS	DHS/USCIS/PIA-007(b) Adoption Case Management System	11/08/2016
USCIS	DHS/USCIS/PIA-003(b) Integrated Digitization Document Management Program (IDDMP)	04/26/2017
USCIS	DHS/USCIS/PIA-067 Civil Surgeon Designation	06/14/2017
USCIS	DHS/USCIS/PIA-009(a) Central Index System (CIS)	04/13/2017
USCIS	DHS/USCIS/PIA-031(a) Comprehensive Immigration Data Repository	01/04/2017
USCIS	DHS/USCIS/PIA-064 myUSCIS	12/21/2016
USCIS	DHS/USCIS/PIA-066 Citizenship and Integration Grant Program	05/23/2017
USCIS	DHS/USCIS/PIA-065Live Chat	05/23/2017

Privacy Impact Assessments Published July 1, 2016 – June 30, 2017		
Component	Name of System	Date Published
USCIS	DHS/USCIS/PIA-031(a) Citizenship & Immigration Data Repository (CIDR)	05/11/2017
USCIS	DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System (CLAIMS 3) and Associated Systems	05/04/2017
USSF	DHS/USSF/PIA-003 Protective Threat Management System (PTMS)	08/29/2016
USSF	DHS/USSF/PIA-012(a) Electronic Name Check System (E-Check)	09/29/2016
USSF	DHS/USSF/PIA-009(a) Field Investigative Reporting System (FIRS)	11/21/2016
USSF	DHS/USSF/PIA-016 Enterprise Person (ePerson) System	02/01/2017
USSF	DHS/USSF/PIA-015(a) eAgent	05/04/2017
USSF	DHS/USSF/PIA-014 Field Support System (FSS)	05/11/2017
USSF	DHS/USSF/PIA-020 Forensic Services Division System (FSDS)	05/11/2017
USSF	DHS/USSF/PIA-018 Laboratory Evidence and Information Management System (LEIMS)	05/26/2017

System of Records Notices Published July 1, 2016 – June 30, 2017		
Component	Name of System	Date Published
CBP	DHS/CBP-001 Import Information System	07/26/2016
CBP	DHS/CBP-022 Electronic Visa Update System (EVUS)	09/01/2016
CBP	DHS/CBP-009 Electronic System for Travel Authorization (ESTA)	4/6/2016
CBP	DHS/CBP-023 Border Patrol Enforcement Records	10/20/2016
CBP	DHS/CBP-007 Border Crossing Information (BCI)	12/13/2016
DHS-Wide	DHS/ALL-014 Personnel Emergency Contact Information	07/26/2016
ICE	DHS/ICE-016 FALCON Search and Analysis	05/05/2017
ICE	DHS/ICE-014 Homeland Security Investigations Forensic Laboratory	07/14/2016
ICE	DHS/ICE-015 LeadTrac	09/12/2016
ICE	DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records	10/19/2016
USCIS	DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE)	11/08/2016
USCG	DHS/USCG/015 Legal Assistance Case Files	07/12/2016
USCG	DHS/USCG-031 USCG Law Enforcement (ULE)	12/08/2016
USCIS	DHS/USCIS-005 - Intercountry Adoptions Security	11/08/2016
USCIS	DHS/USCIS-007 Benefit Information System	10/19/2016
USCIS	DHS/USCIS-017 Refugee Case Processing and Security Screening	10/19/2016