Department of Homeland Security

2019 Privacy Office Annual Report to Congress

For the period July 1, 2018 – June 30, 2019

October 22, 2019

Homeland Security

Message from the Chief Privacy Officer

October 22, 2019

I am pleased to present the Department of Homeland Security Privacy Office's *2019 Annual Report to Congress,* highlighting the achievements of the Privacy Office from July 2018 through June 2019.

The DHS Privacy Office had another productive and busy year, working closely with privacy professionals in the operational Components to implement six new goals articulated in our Strategic Plan for Fiscal Years 2019-2022. This year's report has been restructured to summarize our accomplishments based on the new plan.

Some key highlights include:

Policy

- I convened new DHS-wide Privacy and FOIA Councils in 2018 to facilitate the policy review process and foster implementation among the Components. The Councils meet monthly and are comprised of Component Privacy and FOIA Officers. They also serve as forums for sharing best practices and coordinating cross-Component challenges and developing solutions.
- We issued a new privacy policy instruction requiring all new and legacy DHS IT systems, programs, and forms to use a unique alternative identifier to the Social Security number (SSN). If there are technological, legal, or regulatory limitations to eliminating the SSN, then privacy-enhancing SSN alternatives must be utilized, such as masking, redacting, or truncating the SSN in digital and hard copy formats.
- Through its participation in the Artificial Intelligence (AI) Policy Coordinating Committee, the Privacy Office was able to advocate for the inclusion of specific provisions that facilitate the identification of privacy and civil liberties issues associated with AI with the February 2019 *Executive Order on Maintaining American Leadership in Artificial Intelligence*. Specifically, requirements were added to address concerns around sharing analytic results and data internally with the Federal Government as well as externally, and the need to identify an AI governance model when privacy-sensitive information is used for AI.

Compliance

- As shown by Privacy Impact Assessments featured in this report, we have been busy this year embedding privacy into priority border security and immigration programs.
- Privacy Office staff continue to identify and mitigate privacy concerns that may arise from the implementation of Executive Order 13780, *Protecting the Nation from Foreign Terrorist Entry into the United States* and other recent proposals for enhanced screening and vetting measures.

Oversight
The DHS Privacy Office conducted a Privacy Compliance Review (PCR) of Section 1367 privacy incidents to assist certain Components to identify and mitigate risks that may occur by inadvertent disclosure of information protected by Title 8, United States Code (U.S.C.), Section 1367, confidentiality and prohibited source provisions. Section 1367 incidents are particularly sensitive given the vulnerability of the population they are meant to protect and the potential legal liabilities for certain violations of the statute. Through this PCR, the Privacy Office examined the Components' privacy protections and made four best practice recommendations to prevent and mitigate future privacy incidents affecting individuals protected by Section 1367.

Freedom of Information Act (FOIA) Technology
The DHS Privacy Office continued its work to modernize and consolidate FOIA IT systems across DHS and is now in the procurement process to purchase a FOIA IT solution that makes powerful e-discovery and computer-assisted redaction technology available to FOIA processors at all Components who choose to use the solution. The solution also allows requesters to electronically submit requests to the system and enables cases to be easily transferred between participating Components, eliminating a significant amount of administrative work. The seamless transfer of cases also allows participating Components to assist if there is a surge in FOIA requests or a need for concentrated backlog reduction efforts as in years past.

Looking Ahead to Fiscal Year 2020

Privacy Policy Assessment Project
The DHS Privacy Office is conducting an evaluation of privacy policies, directives, and instructions to ensure compliance with current organizational requirements, that technical content is updated and accurate, and that policies are in line with updated legislative requirements, including citation updates. Next steps in the multi-phase project evaluation include preparing updates to the first set of identified policies, directives, and instructions and migrating existing privacy memoranda to directives or instructions to better facilitate use and reference. Future phases will include implementing processes to conduct interval-based reviews, ascertaining whether the current policy inventory addresses Privacy Office operational needs, and developing a formal communications and implementation strategy for existing and new policies, directives, and instructions.

Use of Advanced Analytics
The DHS Privacy Office is leveraging operational tools that identify and evaluate privacy equities associated with advanced analytics and exploring how to utilize these tools to meet mission needs. Planned development of an advanced analytics assessment tool enables privacy professionals in Headquarters and the Components to communicate more effectively with technologists and analytic developers to build a culture of privacy from the outset. Having knowledge of human oversight, transparency, accuracy, accountability, and diversity impacts related to advanced analytic algorithms facilitates more accurate information sharing agreements, privacy protections, transparency, and notice to users and providers of data.

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

Sincerely,

Jonathan R. Cantor
Chief Privacy Officer, Acting
U.S. Department of Homeland Security

Pursuant to congressional notification requirements, this report is being provided to the leadership of the following congressional committees:

The Honorable Ron Johnson
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Gary Peters
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Lindsey Graham
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 Bennie G. Thompson
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Mike Rogers
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Elijah Cummings
Chairman, U.S. House of Representatives Committee on Oversight and Reform

The Honorable Jim Jordan
Ranking Member, U.S. House of Representatives Committee on Oversight and Reform

The Honorable Jerry Nadler
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable Doug Collins
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Adam Schiff
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Devin Nunes
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

Executive Summary

The Department of Homeland Security (DHS) Privacy Office (Privacy Office) supports all six goals articulated in the DHS Strategic Plan for Fiscal Years (FY) 2020-2024: (1) counter terrorism and homeland security threats; (2) secure U.S. borders and approaches; (3) secure cyberspace and critical infrastructure; (4) preserve and uphold the nation's prosperity and economic security; (5) strengthen preparedness and resilience; and (6) champion the DHS workforce and strengthen the Department.

To accomplish these key objectives, the Privacy Office established six goals in its Strategic Plan for Fiscal Years 2019 - 2022, each supported by specific and measurable objectives, and explained in the chapters that follow:

- **Goal One (*Privacy and Disclosure Policy*)**: Develop and enforce sound privacy and disclosure policies that safeguard personal information, promote information risk management and mitigation, and provide transparency into the Department's activities;
- **Goal Two (*Compliance and Oversight*)**: Ensure the Department preserves and implements privacy protections; complies with privacy and disclosure laws, policies, and regulations; and performs thorough oversight and governance evaluations;
- **Goal Three**: ***(Privacy Best Practices):*** Integrate privacy best practices into Department operations and processes;
- **Goal Four *(FOIA Compliance)***: Provide timely disclosures pursuant to the FOIA, improve responsiveness, and reduce the number and age of pending open FOIA requests;
- **Goal Five *(Outreach, Education, and Reporting)***: Engage with internal and external stakeholders through training, education, and outreach to strengthen privacy and disclosure activities; and
- **Goal Six *(Business Operations)***: Efficiently manage business operations, office workflow, human capital, technology, procurement, financial actions, and resilience to ensure the office is fully supported in carrying out its mission.

Key Privacy Office achievements during the reporting period[1] are listed by strategic goal below. More details on each of these items, and additional achievements, can be found in the body of the report.

Goal One: Privacy and Disclosure Policy

- Issued a new privacy policy instruction requiring all new or legacy DHS IT systems, programs, and forms to use a unique alternative identifier to the SSN. If there are technological, legal, or regulatory limitations to eliminating the SSN, then privacy enhancing SSN alternatives must be utilized, such as masking, redacting, or truncating the SSN in digital and hard copy formats.
- Convened a new DHS Privacy Council, chaired by the Chief Privacy Officer (CPO), to facilitate the privacy policy review process and foster implementation among the Components. The Council, comprised of Component Privacy Officers, is also a forum

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

for sharing privacy best practices and coordinating cross-Component challenges and developing solutions.

Goal Two: Compliance and Oversight

- Approved 53 new or updated Privacy Impact Assessments (PIA) and 10 System of Records Notices (SORN), resulting in a Department-wide Federal Information Security Modernization Act (FISMA) privacy score of 99 percent for required investment technology system PIAs and 100 percent for SORNs.
- Completed three Privacy Compliance Reviews (PCR), oversaw implementation of recommendations from six previous PCRs, and launched two new PCRs. See page 39 for the implementation status of all PCR recommendations.
- Hosted the second annual DHS Privacy Incident Tabletop Exercise in Washington, DC. The exercise was conducted jointly with the Component Security Operations Centers (SOC), led by the Enterprise SOC (ESOC) management team. The Federal Emergency Management Agency's (FEMA) National Exercise Division facilitated the exercise, with privacy representatives from all DHS Components in attendance. The goal of this annual exercise is to refine and validate the breach response plan in the Privacy Incident Handling Guidance (PIHG) and the Major Cybersecurity Incident Response Guide through a simulation and to identify any potential gaps or weaknesses in the breach response process at both the Component and enterprise levels.
- Worked with the HQ IT Service Desk to create a new online portal to make it easier for staff to report privacy incidents, resulting in an increase in employees contacting the Privacy Office to discuss suspected incidents.
- Reviewed 251 raw intelligence information reports (IIR) and draft intelligence reports (FINTEL), 17 briefing packages, and 267 Requests for Information (at all levels of classification). The Privacy Office's product review function is an ongoing, real-time operational service for the Department, requiring around-the-clock monitoring of communications and quick response to the Office of Intelligence and Analysis' (I&A) requests for review of intelligence products.

Goal Three: Privacy Best Practices

- **Insider Threat Program (ITP)**: Privacy Office staff continues to 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. 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.

Goal Four: FOIA Compliance

- Received an eight percent increase in requests from FY 2017 to 2018 – increasing from 366,036 to 395,751 – and processed a record-setting 374,945 requests – a two percent increase from FY 2017.
- Launched an aggressive backlog reduction effort in collaboration with OBIM, CBP, and ICE, which helped eliminate about 12,000 requests from the backlog by the end of FY 2018.
- Issued FOIA policy Instruction 262-11-002, *Freedom of Information Act Reporting Requirements*, to formalize and clarify roles and responsibilities in weekly, monthly, and annual reporting and in the one-day notification process for significant requests.
- Convened the initial meeting of the new DHS FOIA Council, chartered in November 2018 to discuss policy and management matters concerning the departmental FOIA Line of Business functions. The Council is also a forum for sharing FOIA best practices and coordinating cross-Component challenges and developing solutions.

Goal Five: Outreach, Education, and Reporting

- Promoted transparency and engaged with the privacy advocacy community, international partners and stakeholders, and the public through workshops, the Privacy Office website, the Federal Privacy Council's Federal Privacy Summit, and Privacy Office leadership and staff appearances at conferences and other fora.
- Hosted periodic informational meetings with members of the privacy advocacy community to inform them of key privacy initiatives throughout the year.
- Participated 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).

Goal Six: Business Operations

- Maximized operational and financial performance by allowing Components to purchase over $1,000,000 in FOIA and privacy support services using current contract vehicles, reducing acquisition administrative costs and creating time and resource efficiencies.
- Leveraged intra-agency agreements with departmental Offices and Components to reimburse the Privacy Office $414,185 for infrastructure and license costs related to FOIAXpress, the web-based application that processes FOIA and Privacy Act requests.
- The Director of National Intelligence presented the *Privacy and Civil Liberties Team of the Year Award* to Privacy Office staff for their contributions to the National Vetting Center Privacy, Civil Rights, and Civil Liberties Working Group.

Privacy Office
2019 Annual Report to Congress
Table of Contents

Authorities and Responsibilities of the Chief Privacy Officer

Major Federal Privacy Laws

The DHS 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), including the *Judicial Redress Act of 2015*: Embodies a code of fair information principles that governs the collection, maintenance, use, and dissemination of personally identifiable information by federal agencies;
- *E-government Act of 2002* (Public Law 107-347): Mandates Privacy Impact Assessments (PIA) for all federal agencies when there are new collections of, or new technologies applied to, personally identifiable information;
- *Freedom of Information Act of 1966* (FOIA), as amended (5 U.S.C § 552): Implements the principles that persons have a fundamental right to know what their government is doing; and
- *Implementing the Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53): Amends the Homeland Security Act to give new authorities to the Chief Privacy Officer (CPO).

Chief Privacy Officer's Statutory Authorities

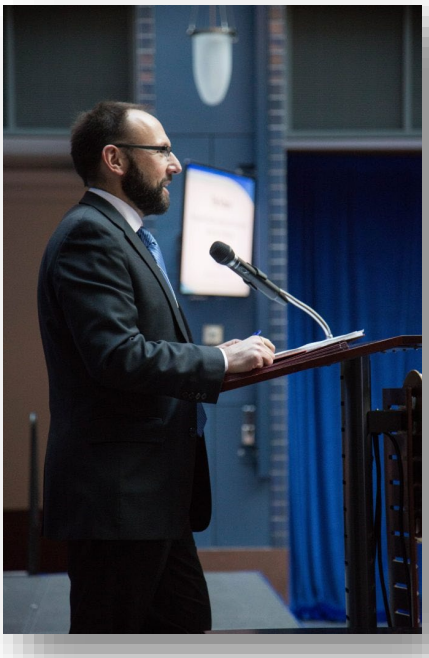
The responsibilities of the CPO are set forth in Section 222 of the *Homeland Security Act of 2002*, as amended:

SEC. 222. [6 U.S.C. 142] PRIVACY OFFICER.
(a) APPOINTMENT AND RESPONSIBILITIES. —The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including—
(1) assuring that the use of technologies sustains, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;
(2) assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
(3) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government;
(4) conducting a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected;
(5) coordinating with the Officer for Civil Rights and Civil Liberties to ensure that—
(A) programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner; and
(B) Congress receives appropriate reports on such programs, policies, and procedures; and

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the Privacy Act of 1974, internal controls, and other matters.
(b) AUTHORITY TO INVESTIGATE.—
(1) IN GENERAL.—The senior official appointed under subsection (a) may—
(A) have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the senior official under this section;
(B) make such investigations and reports relating to the administration of the programs and operations of the Department as are, in the senior official's judgment, necessary or desirable;
(C) subject to the approval of the Secretary, require by subpoena the production, by any person other than a Federal agency, of all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence necessary to performance of the responsibilities of the senior official under this section; and
(D) administer to or take from any person an oath, affirmation, or affidavit, whenever necessary to performance of the responsibilities of the senior official under this section. 7 ‘‘
(2) ENFORCEMENT OF SUBPOENAS.—Any subpoena issued under paragraph (1)(C) shall, in the case of contumacy or refusal to obey, be enforceable by order of any appropriate United States district court.
(3) EFFECT OF OATHS.—Any oath, affirmation, or affidavit administered or taken under paragraph (1)(D) by or before an employee of the Privacy Office designated for that purpose by the senior official appointed under subsection (a) shall have the same force and effect as if administered or taken by or before an officer having a seal of office.
(c) SUPERVISION AND COORDINATION.—
(1) IN GENERAL.—The senior official appointed under subsection (a) shall—
(A) report to, and be under the general supervision of, the Secretary; and
(B) coordinate activities with the Inspector General of the Department in order to avoid duplication of effort.
(2) COORDINATION WITH THE INSPECTOR GENERAL.—
(A) IN GENERAL.—Except as provided in subparagraph (B), the senior official appointed under subsection (a) may investigate any matter relating to possible violations or abuse concerning the administration of any program or operation of the Department relevant to the purposes under this section.
(B) COORDINATION.—
(i) REFERRAL.—Before initiating any investigation described under subparagraph (A), the senior official shall refer the matter and all related complaints, allegations, and information to the Inspector General of the Department.
(ii) DETERMINATIONS AND NOTIFICATIONS BY THE INSPECTOR GENERAL.—
(I) IN GENERAL.—Not later than 30 days after the receipt of a matter referred under clause (i), the Inspector General shall—
(aa) make a determination regarding whether the Inspector General intends to initiate an audit or investigation of the matter referred under clause (i); and
(bb) notify the senior official of that determination.
(II) INVESTIGATION NOT INITIATED.—If the Inspector General notifies the senior official under sub clause (I)(bb) that the Inspector General intended to initiate an audit or investigation, but does not initiate that audit or investigation within 90 days after providing that

notification, the Inspector General shall further notify the senior official that an audit or investigation was not initiated. The further notification under this sub clause shall be made not later than 3 days after the end of that 90-day period.
(iii) INVESTIGATION BY SENIOR OFFICIAL.—The senior official may investigate a matter referred under clause if—
(I) the Inspector General notifies the senior official under clause (ii)(I)(bb) that the Inspector General does not intend to initiate an audit or investigation relating to that matter; or
(II) the Inspector General provides a further notification under clause (ii)(II) relating to that matter.
(iv) PRIVACY TRAINING.—Any employee of the Office of Inspector General who audits or investigates any matter referred under clause (i) shall be required to receive adequate training on privacy laws, rules, and regulations, to be provided by an entity approved by the Inspector General in consultation with the senior official appointed under subsection (a).
(d) NOTIFICATION TO CONGRESS ON REMOVAL.— If the Secretary removes the senior official appointed under subsection (a) or transfers that senior official to another position or location within the Department, the Secretary shall—
(1) promptly submit a written notification of the removal or transfer to Houses of Congress; and
(2) include in any such notification the reasons for the removal or transfer.
(e) REPORTS BY SENIOR OFFICIAL TO CONGRESS.—The senior official appointed under subsection (a) shall—
(1) submit reports directly to the Congress regarding performance of the responsibilities of the senior official under this section, without any prior comment or amendment by the Secretary, Deputy Secretary, or any other officer or employee of the Department or the Office of Management and Budget; and
(2) inform the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives not later than—
(A) 30 days after the Secretary disapproves the senior official's request for a subpoena under subsection (b)(1)(C) or the Secretary substantively modifies the requested subpoena; or
(B) 45 days after the senior official's request for a subpoena under subsection (b)(1)(C), if that subpoena has not either been approved or disapproved by the Secretary.

DHS Privacy Office Overview



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

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

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

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

Who We Serve

The Privacy Office serves the Department, other federal agencies, the American people, immigrants, and visitors to the United States.

Privacy Office Mission

The Privacy Office enables the Department to accomplish its mission while protecting individuals' privacy and facilitating public disclosure.

The DHS Privacy Office also:

- Works with every Component and program in the Department to ensure privacy considerations are addressed when planning or updating any program, system, form, or initiative that may use PII.
- Evaluates legislative and regulatory proposals involving the collection, use, and disclosure of PII;

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

DHS Fair Information Practice Principles

The Fair Information Practice Principles (FIPP),[2] shown in Figure 1, are the cornerstone of DHS's efforts to integrate privacy and transparency into all operations in tandem with *DHS Privacy Policy 2017-01 Regarding the Collection, Use, Retention, and Dissemination of Personally Identifiable Information*.

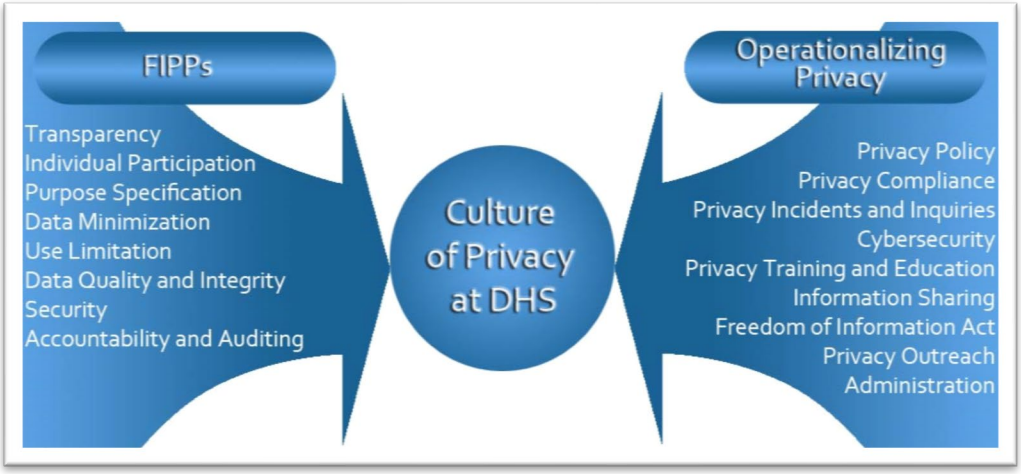


Figure 1: Privacy Office Implementation of the FIPPs

The Privacy Office incorporates these well-recognized principles into privacy and disclosure policy and compliance processes throughout the Department. The Privacy Office also undertakes statutory and policy-based responsibilities in collaboration with Component privacy officers,[3] privacy points of contact (PPOC),[4] Component FOIA Officers, and program offices to

[2] 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

[3] 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.*

[4] 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.

ensure all privacy and disclosure issues are afforded the appropriate level of review and expertise.

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

Privacy Office Structure

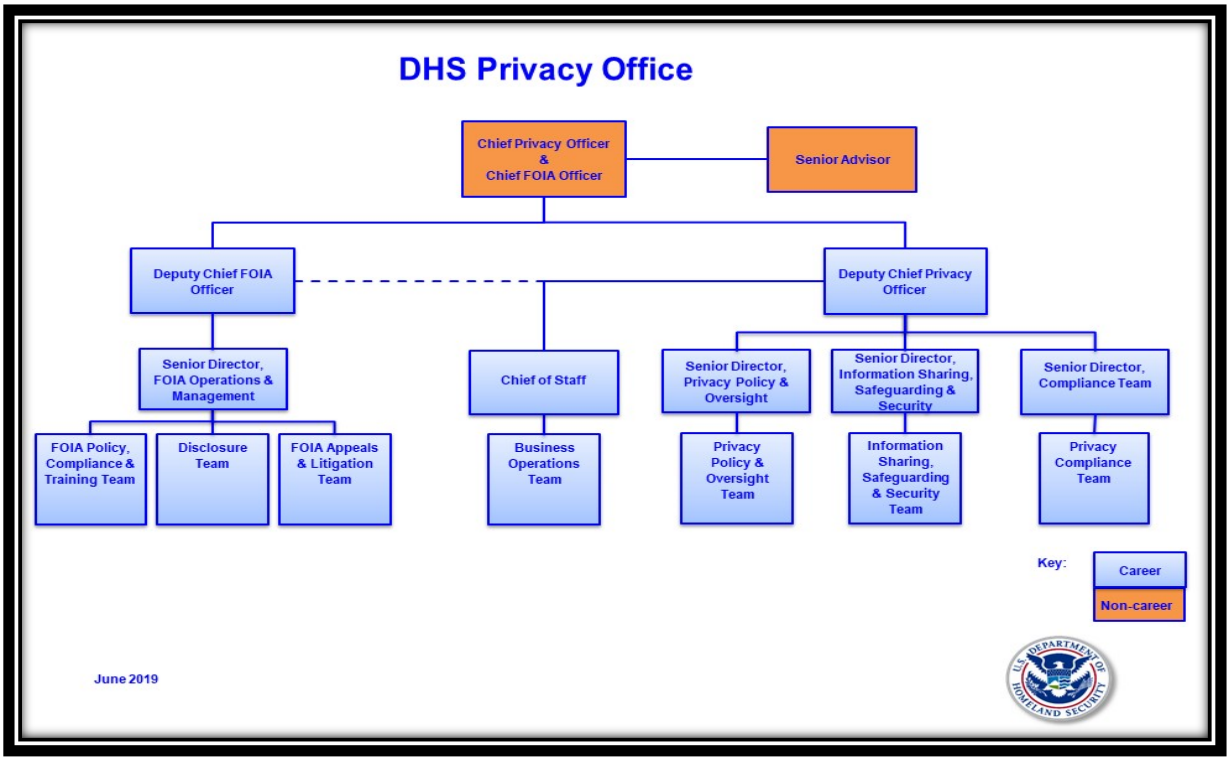


Figure 2: Privacy Office Organizational Chart[5]

The DHS Privacy Office is composed of five teams:

1) **The Privacy Policy and Oversight Team** bears primary responsibility for developing DHS privacy policy, as well as providing subject matter expertise and support for policy development throughout the Department in areas that impact individual privacy. These areas include social media, "big data," enterprise data management, cybersecurity, acquisitions and procurement, and international engagement. This team is dedicated to implementing accountability and continually improving DHS privacy processes and programs, such as in the development of the National Vetting Center (NVC), established by National Security Presidential Memorandum (NSPM) - 9. This team also conducts PCRs 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.

[5] As of the date of publication, the Deputy Chief Privacy Officer is acting as the Chief Privacy Officer.

2) **The Privacy Compliance Team** oversees privacy compliance activities, which includes supporting DHS Component privacy officers, PPOCs, and DHS programs. Examples of compliance activities include reviewing Privacy Threshold Analyses (PTA), PIAs, SORNs, 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[6] (IC) as well as immigration and law enforcement partners at the federal, state, local, tribal, territorial, and international level. The team engages with operational, policy, and oversight stakeholders—both within DHS and with other federal partners—throughout the information sharing lifecycle. The team accomplishes this by evaluating information sharing requests, assessing and mitigating privacy risks, and reviewing compliance with internal policies and agreement privacy terms and conditions. Team members participate in Privacy Office efforts to review intelligence products and Component-implemented intelligence rules, provide intelligence-related privacy training, and provide policy guidance for other related DHS initiatives. This includes, but is not limited to, safeguarding information, preventing insider threats, countering violent extremism, the deployment of unmanned aircraft systems (UAS), and the sharing of biometric data, both domestically and internationally. The team also ensures DHS compliance with the *Computer Matching and Privacy Protection Act of 1988*.

4) **The FOIA Team** oversees Department-wide FOIA operations and policy. The team comprises three groups: Disclosure; FOIA Policy, Compliance, and Training; and FOIA Appeals and Litigation.

   - The Disclosure Team is responsible for receiving, tracking, processing, and closing all FOIA requests received by the Privacy Office. The team processes initial FOIA and Privacy Act requests for the offices under the purview of the Office of the Secretary.[7] The team is also responsible for engaging with the Components on the proper handling and processing of all FOIA transfers and referrals to DHS Privacy Office.
   - The FOIA Policy, Compliance, and Training Team is responsible for developing FOIA resource guidance and training materials for FOIA professionals and DHS employees. The team ensures Departmental and Component guidance is in compliance with FOIA/Privacy Act policies and procedures while promoting transparency. The team is

[6] A succinct definition is available on: www.dni.gov.

[7] In this report, a reference to the "Department" or "DHS" means the entire Department of Homeland Security, including its Components, Directorates, and the Office of the Secretary. The DHS FOIA Office processes the Privacy Office's initial requests and those for the following offices: Office of the Secretary, Military Advisor's Office, Office of the Citizenship and Immigration Services Ombudsman, Office of the Executive Secretary, Office of Partnership and Engagement, Management Directorate, Office for Civil Rights and Civil Liberties, Office of Operations Coordination, Office of Strategy, Policy, and Plans, Office of the General Counsel, Office of Legislative Affairs, and Office of Public Affairs. In December 2017, DHS established the Countering Weapons of Mass Destruction Office (CWMD) that consolidated the Domestic Nuclear Detection Office (DNDO) and a majority of the Office of Health Affairs, as well as other DHS functions, into CWMD.

also responsible for completing required annual reports and regularly providing detailed statistical analyses of DHS-wide FOIA operations.
- The FOIA Appeals and Litigation Team serves as liaison between the Office of the General Counsel (OGC) and the Privacy Office leadership on complex FOIA requests. The team provides guidance and training on recent developments in the field of disclosure, including court decisions and current legislation. The team researches, analyzes, and evaluates complex FOIA requests to determine if the FOIA and Privacy Act were properly applied during the original processing of a FOIA request.

5) **The Business Operations Team e**fficiently manages business operations, office workflow, human capital, technology, procurement, financial actions, and resilience to ensure the office is fully supported in carrying out its mission.

Working with the DHS Privacy Office

Department personnel:

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

Privacy advocates and the public:

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

International partners:

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

I. Privacy and Disclosure Policy

The Privacy Office's FY 2019-2022 Strategic Plan includes:

Goal One (Privacy and Disclosure Policy): Develop and enforce sound privacy and disclosure policies that safeguard personal information, promote information risk management and mitigation, and provide transparency into the Department's activities.

This chapter highlights the Privacy Office's development and support of new and ongoing policy initiatives to promote privacy and transparency 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 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 the use of technology sustains, and does not erode, privacy protections relating to collection, use, dissemination, and maintenance of PII. The Privacy Office also provides 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, privacy incident response, cybersecurity, acquisitions and procurement, and intelligence products.

All DHS privacy policies are available online at: https://www.dhs.gov/policy
In September 2018, the CPO stood up a new DHS Privacy Council, chaired by the CPO, to facilitate the privacy policy review process and foster implementation among Components. The Council, comprised of Component Privacy Officers, is also a forum for sharing privacy best practices and coordinating cross-Component challenges and developing solutions.

New or Revised Privacy Policies

New: *Social Security Number Collection and Use Reduction Instruction*
This new privacy policy replaces the 2007 policy requiring system owners to have statutory or regulatory authority to collect and use Social Security Numbers (SSN). This policy goes further, requiring that:

1. System owners, *even if their system is properly authorized to collect SSNs*, use an alternative identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, the Privacy Office requires privacy-enhancing alternatives, such as masking/truncating the SSN or blocking the display of SSNs on paper forms, correspondence, and computer screens. This is also mandated by Office of Management and Budget (OMB) *Circular Number A-130: Managing Federal Information as a Strategic Resource*.
2. Approved DHS-specific forms containing SSNs mailed through the United States Postal Service must have the SSN masked, truncated, redacted, or be sent via a secure method.

DHS has developed a unique alternative identifier to mask employee and contractor SSNs in human capital systems. Additional unique alternative identifiers are needed to replace SSNs collected from the public. As of June 2019, DHS maintains an inventory of approximately 700 programs, systems, and forms authorized to collect and use the SSN, including human capital systems.

Details on FOIA policies can be found in Chapter 4.

Privacy Policy Leadership

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

Acquisition Regulations and Departmental Policies

The Privacy Office is involved in four separate interagency Federal Acquisition Regulation (FAR) efforts:

1. The first effort involves the ongoing work to implement a FAR clause to address the reporting requirements of OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*. This clause requires contractors and subcontractors who collect, maintain, use, share, or dispose of PII on behalf of the government to provide adequate security and privacy protections for such information, and rapidly report any breach in accordance with the clause. Development of the FAR clause was the first step in the implementation process. Oversight efforts continue until the clause is incorporated into the FAR and included in all applicable DHS contracts and agreements.

2. The Privacy Office continues to take part in an interagency working group to amend the FAR to implement the Federal Controlled Unclassified Information (CUI) Program. The CUI program affects all organizations that handle, possess, use, share, or receive CUI, including federal contractors. The Privacy Office continues to support this effort while ensuring that sensitive information, including PII, is appropriately safeguarded throughout the data lifecycle.

3. Homeland Security Acquisition Regulation (HSAR) Class Deviation 15-01 enforcement activities continue to heighten protection of sensitive information and information systems where they reside. Enforcement activities focus on ensuring that program offices coordinate with the Privacy Office when deciding to include or exclude the special clauses in contracts and solicitations. In addition, DHS has deployed training that addresses the requirements of the HSAR Class Deviation and expectations for implementation, including mandatory coordination with impacted stakeholders and subject matter experts (SME).

4. The Privacy Office was part of a departmental effort to design and implement a process to determine when a stop work order for DHS contracts should be issued (and later lifted) after receiving an incident notification. This process also identifies whether all or part of the contractor's scope of work is affected during the stop work period. The Privacy Office's focus throughout design and implementation was the preservation of forensic information and the ability to work with the contractor to investigate, mitigate, and remediate a privacy incident, pursuant to OMB guidance and DHS policy.[8]

[8] See OMB M-17-12 and OMB M-19-02, and DHS Privacy Policy Instruction 047-01-006 Privacy Incident Responsibilities and Breach Response Team, DHS Privacy Policy Instruction 047-01-007 Handbook for Safeguarding Sensitive PII, and DHS Privacy Policy Instruction 047-01-008 Privacy Incident Handling Guidance.

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.

Cybersecurity

The Privacy Office is actively engaged in interagency cybersecurity policy initiatives and programs to integrate privacy protections into cybersecurity activities and embed privacy safeguards into the technologies and processes deployed for cyber detection and prevention. This support and involvement also extends to the review of privacy compliance documentation related to DHS cyber programs that oversee the Data Privacy and Integrity Advisory Committee's (DPIAC) cyber subcommittee.

Executive Order 13636/13691 Privacy and Civil Liberties Assessments Report

The Privacy Office and Office for Civil Rights and Civil Liberties (CRCL) continue to collaborate and coordinate between Agencies to draft and publish the annual *Executive Order 13636/13691 Privacy and Civil Liberties Assessments Report*. This Report requires senior agency officials for privacy (SAOP) and civil liberties to assess the privacy and civil liberties impacts their activities have on Executive Orders (EO) implementation and to publish their assessments annually in a report compiled by the Privacy Office and CRCL.

Privacy and Civil Liberties Oversight Board (PCLOB) Machine Learning Working Group

On May 7, 2019, the PCLOB held its kick-off meeting to establish its Machine Learning Working Group. In addition to PCLOB members and staff, the Working Group is comprised of SAOPs and civil liberties officials from the interagency and their staffs, with an intent of "producing a framework that reflects interagency consensus on privacy and civil liberties principles in machine learning development, acquisitions, and use in national security and law enforcement contexts." The scope of the Working Group is to develop a set of principles for the use of machine learning tools in an Intelligence Community (IC) setting, reducing bias in machine learning data set training, and determining how to purge data without affecting the utility of the algorithms.

Executive Order on Maintaining American Leadership in Artificial Intelligence (AI)

Through participation in the AI Policy Coordinating Committee (PCC), the Privacy Office advocates for the inclusion of specific provisions that facilitate the identification of privacy and civil liberties issues associated with AI with the February 2019 EO. Specifically, requirements were added to address concerns around sharing analytic results and data internally with the Federal Government and externally. Another requirement involves the need to identify an AI governance model when privacy-sensitive information is used for AI. Since the Presidential signing, focus has now shifted to the associated AI Implementation Plan. The DHS Privacy Office's equities in the AI Implementation Plan include identifying the privacy issues most likely to arise in an AI context, policy approaches to mitigate those issues, parameters on data and results sharing (especially in the Research and Development context), and how to facilitate AI Governance and Oversight within federal agencies.

Privacy Office Advanced Analytics (AA) Cross Functional Team
The increasing use of AA at DHS necessitates a holistic approach to address privacy policy, oversight, and governance. To that end, a Privacy Office AA Cross Functional Team was established in 2018. This team is comprised of individuals from the Privacy Office's Compliance, Information Sharing, Security, and Safeguarding (IS3), and Policy and Oversight staffs to evaluate and develop an enterprise-wide AA governance structure. Engagement with the Component Privacy Offices and other agencies is essential to identify and define AA. Activities under consideration for the functional team include modifying privacy documentation and reports to accurately capture AA use, issuing policy to define parameters on use with privacy sensitive information, and determining if an Analytic Review Board (ARB) should be convened to oversee deployment.

Mission Number Four: Safeguard and Secure Cyberspace.

Data Framework

Currently, the vision of the DHS Data Framework is to become a center of excellence for customized data services to help generate insights and value of data. The mission of the Data Framework is to provide infrastructure, tools, and knowledge to deliver data analytics capabilities and services for HQ entities and other DHS Components.

In 2018, the Data Framework completed a critical refresh project establishing a strong foundational enterprise data management platform bringing enhanced capabilities to Framework users. These capabilities include high speed, high quality data through near real time data processing; an advanced ability to identify record changes and updates; and data flow monitoring. Additionally, the refresh brought improved system performance and the ability to support future growth and increased data volumes. The Data Framework completed its unclassified use project, which allowed users to access data directly from the unclassified environment, also known as Neptune. Neptune continues to build in privacy protections while enabling a more controlled, effective, and efficient use of existing homeland security-related information.

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

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

Also, in 2018, the *DHS Data Framework Act of 2018*[9] (Act) directed the Department, within two years, to:

(1) Develop a data framework to integrate existing DHS datasets and systems for access by authorized personnel in a manner consistent with relevant legal authorities and privacy, civil rights, and civil liberties protections;
(2) Validate all information of a DHS office or component that falls within the scope of the information sharing environment and any information or intelligence relevant to priority mission needs and capability requirements of the homeland security enterprise is included; and
(3) Ensure the framework is accessible to DHS employees who have an appropriate security clearance, who are assigned to perform a function that requires access, and who are trained in applicable standards for safeguarding and using such information.

Legislative compliance recommendations and proposals are being developed to implement all aspects of the 2018 Legislation within the two-year timeframe.

The Privacy Office performs a significant oversight role as datasets are prioritized, tagged, and moved into the Data Framework and as new analytical tools are deployed and remains intensively involved in onboarding users, new data, and new capabilities within the program. The DHS Privacy Office continues to evaluate the need for updated PIAs and remains involved in the development of governance structures as the Data Framework changes its operating model and matures.

Mission Number One: Prevent Terrorism and Enhance Security.

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, codifying an existing relationship between DHS and a national network of fusion centers. The Privacy Office exercises leadership by 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 they are as comprehensive as the *Information Sharing Environment (ISE) Privacy Guidelines* and assists fusion centers with incorporating privacy protections in new policies and templates, such as facial recognition and automated license plate readers. The Privacy Office also collaborates with CRCL and DHS Intelligence and Analysis's (I&A) State and Local Partner Engagement Office to train fusion center privacy officers and analytical staff.

Mission Number One: Prevent Terrorism and Enhance Security.

[9] Pub. L. No. 115-331 (Dec. 19, 2018).

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, CRCL, 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 may pose an insider threat. DHS Privacy Office staff are also working with other members of the ITOG to finalize auditing procedures. The ITWG helps 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 (SME) 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. This year, Privacy Office staff worked closely with ITP leadership to start expanding the ITP to cover threats other than the inappropriate disclosure of classified information and to include non-cleared DHS personnel.

Mission Number One: Prevent Terrorism and Enhance Security.

Joint Requirements Council

The Privacy Office supports the Joint Requirements Council (JRC), which reports to the Deputy Secretary's Management Action Group (DMAG) and serves as an executive level body that provides oversight of the DHS operational requirements generation process, harmonizes efforts across the Department, and makes prioritized funding recommendations to the DMAG for those validated operational requirements. The JRC is also responsible for examining what tools and resources the Department needs 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 CPO and the Deputy CPO participate in the DMAG, as needed.

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.

Screening and Vetting Initiatives

To identify and mitigate privacy concerns that may arise from the implementation of EO 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 participates in several intra- and inter-agency working groups and meetings. Two such initiatives are associated with NSPM-7 and NSPM-9.

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

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

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

NSPM-9, *Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise (NVE)*, issued February 6, 2018, directed the Secretary of Homeland Security, in coordination with the Secretary of State, the Attorney General, and the Director of National Intelligence, to establish the NVC. The NVC improves efficiency and effectiveness of U.S. Government vetting programs to better identify individuals who may pose a threat to national security, border security, homeland security, or public safety, consistent with law and policy. NSPM-9 establishes a policy to use intelligence and law enforcement information, as authorized by existing law, in support of adjudications or other decisions involved in immigration and border security missions.

The Privacy Office is directly engaged in oversight and governance efforts related to NSPM-9 and the on-going activities of the NVC. From an operational perspective, the NVC Board serves as the senior interagency forum for considering issues that affect the national vetting enterprise and the activities of the Center. In furtherance of oversight and governance, there is a Privacy, Civil Rights and Civil Liberties (P-CRCL) Working Group, which is comprised of senior privacy and civil liberties officials from several departments and agencies supporting the implementation of NSPM-9.

This Working Group ensures the activities of the NVC Governance Board and NVC appropriately protect individuals' privacy, civil rights, and civil liberties. The Working Group also provides specific advice and guidance to the NVC and the Governance Board on privacy and civil liberties issues. DHS's CPO serves as a co-chair of the P-CRCL Working Group and represents the P-CRCL Working Group as an *ex officio*, non-voting member of the Governance Board. Privacy Office staff are also members of the Working Group, which meets regularly to evaluate screening and vetting program proposals, the attendant Implementation Plans, Concepts of Operations, and technology structures to ensure NVC activities are being conducted in a privacy-protective manner. To further support privacy oversight and governance, the NVC staffed a P-CRCL Officer, who reports to the P-CRCL co-chairs, to incorporate privacy, civil rights, and civil liberties protections into all aspects of planning and implementation for the NVC.

Mission Number One: Prevent Terrorism and Enhance Security.

Terrorist Prevention Working Group (TPWG)

The Privacy Office is involved in terrorism prevention activities primarily through participation in the Office of Terrorism Prevention's Terrorism Prevention Working Group (formerly Countering Violent Extremism Working Group). Staff reviews research and programs and work product prior to completion to ensure the Department's terrorism prevention work is consistent with applicable privacy law and policy.

Mission Number One: Prevent Terrorism and Enhance Security.

Unmanned Aircraft Systems (UAS)

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

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

The Privacy Office works with CRCL to evaluate SLTT requests to use preparedness grant funding administered by the FEMA Grant Programs Directorate to acquire sUAS, as required by the Presidential Memorandum on *Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (Section 1(c)(vi)). The Privacy Office, in concert with CRCL, reviewed approximately thirty such requests during the current reporting period. Several submissions are on hold pending receipt of additional material at the request of the Privacy Office. Most submissions are cleared after applicants revise their policies or submit additional material. The Privacy Office devotes significant attention to ensure robust privacy protections are in place for all grant applicants intending to operate sUAS. In all cases, we provide SLTT agencies with links to the *Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft Systems Programs* and the "Presidential Memorandum" for their use in further developing their programs.

The Preventing Emerging Threats Act of 2018[10] authorizes DHS to employ CUAS in specific circumstances and establishes processes and procedures that must be followed before operating Counter-UAS Technology. This Act also requires privacy protections that go beyond the Privacy Act. Privacy Office staff serve on the CUAS Executive Steering Committee (ESC) and all Department-level CUAS working groups and sub-working groups. The ESC and subordinate working groups determine appropriate methods and policies to interdict, redirect, or otherwise interrupt the flight of UAS encroaching on restricted airspace, hazarding protective operations, or potentially causing harm to critical infrastructure or key resources. There is a perceived risk that

[10] Division H of the FAA Reauthorization Act of 2018, Pub. L. No. 115-254.

counter-UAS operations might interfere with the innocent flight of sUAS, and during such counter-UAS operations, DHS might gain access to PII.

The Privacy Office is diligently working with its partners to develop suitable policies and procedures to minimize the possibility that a DHS Component would inappropriately gain access to a person's PII. Privacy Office staff are also directly working with the Components to build-in privacy protections at the exact locations where CUAS may be deployed. For example, DHS S&T published a PIA in November 2018 discussing measures taken to mitigate privacy risks and protect PII during DHS S&T's testing and evaluation of C-UAS technologies.

Mission Number Two: Secure and Manage Our Borders.

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

In the 2018 *Consolidated Appropriations Act*,[11] Congress provided the Privacy Office with additional funding to ensure information and data released by the Department does not reveal the identity or PII of non-U.S. Persons who may be survivors of domestic violence, sexual assault, stalking, human trafficking, or other crimes. The confidentiality protections afforded to alien victims of crimes are statutorily required under Title 8, United States Code, Section 1367, *Violence Against Women Act* (herein Section 1367). The DHS Officer for CRCL has, through Secretarial delegation, the authority to provide DHS-wide guidance and oversight on the implementation of Section 1367 confidentiality and prohibited source provisions. The CPO must determine any potential impacts a privacy incident may have on the privacy of individuals, including those protected by Section 1367. Because of the shared responsibilities for ensuring the proper handling of Section 1367 information, in FY 2018 the Privacy Office and CRCL developed a process for the two offices to share incidents of unauthorized Section 1367 disclosures and partner to ensure incidents are appropriately reviewed, investigated, addressed, and resolved.

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

In May 2018, the CPO initiated a PCR of Privacy Incidents Affecting Individuals Protected by Section 1367, focused on those Components and offices most likely to access or be responsible for dissemination of Section 1367 records: United States Immigration and Customs Enforcement (ICE), CBP, U.S. Citizenship and Immigration Services (USCIS), the Cybersecurity and Infrastructure Security Agency's (CISA) Office of Biometric Identity Management (OBIM), and I&A. The PCR, entitled *Privacy Incidents Affecting Individuals Protected by Section 1367,* was completed on February 4, 2019. The findings are intended to provide a means to improve compliance and further enhance the privacy-protective processes for Section 1367 information.

[11] Pub.L. 115-141

The PCR's findings and recommendations are discussed in detail in the Privacy Compliance Review section of this report.

The CPO also reviewed relevant PIAs and ISAAs to ensure the inclusion of language to protect Section 1367 records. The Privacy Office is also developing instructions to disseminate to FOIA professionals that outline withholding requirements of this information.

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

II. Compliance & Oversight

The Privacy Office's FY 2019-2022 Strategic Plan includes:

Goal Two (Compliance and Oversight): Ensure the Department preserves and implements privacy protections; complies with privacy and disclosure laws, policies, and regulations; and performs thorough oversight and governance evaluations.

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, programs and services can provide the maximum public benefit with the lowest possible privacy risk.

Privacy Compliance

The Privacy Office ensures 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. The Privacy Office assesses the privacy risk of Departmental programs and develops mitigation strategies by reviewing and approving all DHS privacy compliance documentation.

The DHS privacy compliance documentation process[12] 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.

The Department's 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 ensures the Department meets statutory requirements such as Federal Information Security Modernization Act of 2014 (FISMA)[13] privacy reporting.

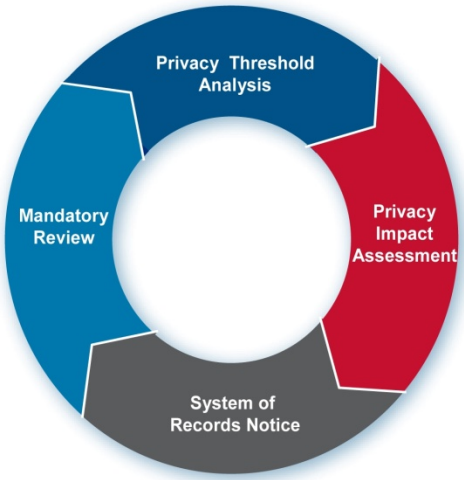


Figure 3: Privacy Office Compliance Process

- At the end of June 2019, the Department's FISMA privacy score showed that 99 percent of FISMA-related systems that required a PIA had a completed PIA in place, and 100 percent of required SORNs have been completed.

[12] See Appendix C for a description of privacy compliance documentation.
[13] 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.

- 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 53 PIAs published online during the reporting period. A complete list sorted by Component can be found in Appendix D.

Listed here are 10 key PIAs approved during this reporting period:

1. DHS/CBP/PIA-056 Traveler Verification Service

Background: CBP is congressionally mandated to deploy a biometric entry/exit system to record arrivals and departures to and from the United States. Following several years of testing and pilots, CBP successfully operationalized and deployed facial recognition technology, now known as the Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in air, land, and sea environments. CBP issued PIAs documenting each new phase of TVS testing and deployment.

Purpose: CBP issued this comprehensive PIA to consolidate all previously issued PIAs and provide notice to the public about how TVS collects and uses personally identifiable information (PII). CBP conducted this overarching, comprehensive PIA for the TVS to replace all previous PIAs and provide a consolidated privacy risk assessment for TVS. *(November 14, 2018)*

2. DHS/CBP/PIA-022(a) Border Surveillance Systems (BSS)

Background: CBP deploys Border Surveillance Systems (BSS) to provide comprehensive situational awareness along the United States border for border security and national security purposes and to assist in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law. BSS includes commercially available technologies such as fixed and mobile video surveillance systems, range finders, thermal imaging devices, radar, ground sensors, and radio frequency sensors.

Purpose: CBP updated this PIA to assess privacy risks associated with new border surveillance technologies not addressed in the original PIA, including maritime and ground radar, enhanced video capabilities, seismic and imaging sensors, and use of commercially available location data to identify activity in designated areas near the United States border. *(August 21, 2018)*

3. DHS/CBP/PIA-058 Publicly Available Social Media Monitoring and Situational Awareness Initiative

Background: CBP takes steps to ensure the safety of facilities and personnel from natural disasters, threats of violence, and other harmful events and activities. In support of these efforts, designated CBP personnel monitor publicly available, open source social media to provide situational awareness and to monitor potential threats or dangers to CBP personnel and facility

operators. Authorized CBP personnel may collect publicly available information posted on social media sites to create reports and disseminate information related to personnel and facility safety.

Purpose: CBP conducted this PIA because, as part of this initiative, CBP may incidentally collect, maintain, and disseminate PII over the course of these activities. *(March 25, 2019)*

4. DHS/ALL/PIA-071 Office of Immigration Statistics (OIS) Statistical Data Production and Reporting

Background: The DHS Office of Immigration Statistics (OIS) is responsible for carrying out two statutory requirements: 1) collecting and disseminating to Congress and the public information useful in evaluating the social, economic, environmental, and demographic impact of immigration laws; and 2) establishing standards of reliability and validity for immigration statistics collected by the Department's operational Components. To meet these requirements, OIS collects immigration-related data from across DHS and other federal immigration agencies, prepares the data for statistical purposes, and creates a variety of statistical products to inform the public, Congress, and Department leadership on key trends in immigration to the United States.

Purpose: OIS conducted this PIA as it collects and uses PII to create its statistical products to inform the public on use of its PII and demonstrate how OIS mitigates privacy risks. *(December 7, 2018)*

5. DHS/ALL/PIA-072 National Vetting Center (NVC)

Background: Through NSPM-9, the President has mandated the Federal Government improve how Executive departments and agencies (agencies) coordinate and use intelligence and other information to identify individuals who present a threat to national security, border security, homeland security, or public safety in accordance with their existing legal authorities and all applicable policy protections. To achieve this mandate, the President directed the establishment of the NVC within DHS, with the purpose of coordinating agency vetting efforts to locate and use relevant intelligence and law enforcement information to identify individuals who may present a threat to the homeland. The Secretary of Homeland Security delegated this responsibility within DHS to CBP.

Purpose: DHS conducted this PIA to assess the risks to privacy, civil rights, and civil liberties presented by the NVC and the vetting programs that will operate using the NVC. *(December 11, 2018)*

6. DHS/ICE/PIA-050 Rapid DNA Operational Use

Background: ICE deployed Rapid DNA technology as a factor to determine if removable aliens who represent themselves as a family unit (FAMU) when apprehended by DHS do, in fact, have a bona fide parent-child relationship. Rapid DNA technology performs a relatively quick (90 minutes), low-cost DNA analysis to meet this need.

Purpose: ICE conducted this PIA for the following reasons:

- To provide transparency about the limited scope of Rapid DNA use, which simply compares two DNA profiles (of the adult and child) to determine whether a parent-child relationship exists;
- To outline the privacy risks involved in using Rapid DNA technology; and
- To explain how ICE will mitigate any risks pertaining to privacy. *(June 25, 2019)*

7. DHS/S&T/PIA-034 Counter Unmanned Aircraft Systems Program

Background: The DHS Science and Technology Directorate (S&T) leads DHS efforts to coordinate across the Federal Government all testing and evaluating technologies used to detect, identify, and monitor small Unmanned Aircraft Systems (sUAS) that may pose a potential threat to covered facilities and assets and other missions authorized by law. These protective technologies are referred to as Counter-UAS (CUAS).

Purpose: DHS S&T conducted this PIA to discuss measures taken to mitigate privacy risks and protect PII during DHS S&T's testing and evaluation of CUAS technologies. *(November 9, 2018)*

8. DHS/TSA/PIA-018(i) Secure Flight Silent Partner and Quiet Skies

Background: The Transportation Security Administration (TSA) leverages its access to the CBP Automated Targeting System (ATS) to identify individuals for enhanced screening during air travel through use of rules based on current intelligence as part of its Secure Flight vetting process. This PIA describes two specific TSA uses of that capability.

1. TSA's Silent Partner program enables TSA to identify passengers for enhanced screening on international flights bound for the United States.
2. Under TSA's Quiet Skies program, TSA uses a subset of Silent Partner rules to identify passengers for enhanced screening on some subsequent domestic and outbound international flights.

The Silent Partner and Quiet Skies programs add another layer of risk-based security by identifying individuals who may pose an elevated security risk in addition to individuals on other watch lists maintained by the Federal Government, so TSA can take appropriate actions to address and mitigate that risk.

Purpose: TSA conducted this PIA update to reflect operational and administrative changes to the TSA Secure Flight Program. *(April 19, 2019)*

9. DHS/USCIS/PIA-076 Continuous Immigration Vetting

Background: USCIS began Continuous Immigration Vetting (CIV) in 2017. To further enhance the agency's ability to identify national security concerns, USCIS vets information from certain immigration benefit applications throughout the entire application adjudication period as new information is received, rather than only performing point-in-time checks. CIV is an event-based vetting tool that automates and streamlines the process of notifying USCIS of potential derogatory information in Government databases that may relate to individuals in USCIS systems as new information is discovered. USCIS is now incrementally expanding CIV to encompass screening and vetting immigrant and nonimmigrant applications and petitions throughout the duration of the benefit or status, until the individual becomes a naturalized U.S. Citizen.

Purpose: USCIS published this PIA to provide greater transparency into the CIV initiative and to assess the impact of automating event-based vetting for individuals from initial benefit filing until naturalization. *(February 14, 2019)*

10. DHS/USSS/PIA-024 Facial Recognition Pilot

Background: USSS will operate a Facial Recognition Pilot (FRP) at the White House Complex to biometrically confirm the identity of volunteer USSS employees in public spaces around the complex. The FRP seeks to test USSS's ability to verify the identities of a test population of volunteer USSS employees. Ultimately, the goal of the FRP is to identify whether facial recognition technologies can assist USSS to identify known subjects of interest prior to initial contact with law enforcement at the White House Complex.

Purpose: Collection of volunteer subject data will assist USSS in testing the ability of facial recognition technology to identify known individuals and to determine if biometric technology can be incorporated into the continuously evolving security plan at the White House Complex. *(November 26, 2018)*

System of Records Notices

The Privacy Office publishes new and updated SORNs on its website: www.dhs.gov/privacy. During the reporting period, the CPO approved 10 SORNs. A complete list sorted by Component can be found in Appendix D.

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

1. DHS/ALL-018 Grievances, Appeals, and Disciplinary Action Records

Background: The DHS Administrative Grievance Records System is a system of records relating to grievances filed by DHS employees under the Administrative Grievance System or under a negotiated grievance procedure. The system contains all documents related to each grievance in the central personnel or administrative office in DHS Headquarters or of the Component or its field offices, where the grievance originated. This system of records creates greater consistency across the Department in the category of individuals, category of records, and routine uses of administrative grievance records.

Purpose: The purpose of this system of records is to collect, maintain, and store information related to administrative grievances filed by current and former DHS personnel. Records are used by the Department to resolve employee concerns about working conditions, the administration of collective bargaining agreements, employee/supervisor relations, work processes, or other similar issues. *(April 29, 2019; 84 FR 18070))*

2. DHS/ICE-017 Angel Watch Program System

Background: ICE's Angel Watch Program is conducted as part of the Angel Watch Center (AWC), a joint initiative among ICE, DHS's CBP, and the U.S. Department of Justice's (DOJ) U.S. Marshals Service, as prescribed by International Megan's Law (IML) to Prevent Child Exploitation and Other Sexual Crimes through Advanced Notification of Traveling Sex Offenders.

Purpose: The purpose of this system is to collect information on covered sex offenders to: (1) Combat transnational child sex tourism or exploitation; (2) Share information with foreign countries on covered sex offenders to aid making informed decisions regarding the admissibility of travelers; (3) Support the receipt of and response to any complaints by alleged covered sex offenders or others related to the activities of the Angel Watch Program; (4) Identify potential criminal activity; (5) Uphold and enforce criminal laws; and (6) Ensure public safety. *(February 1, 2019; 84 FR 1182))*

3. DHS/TSA-001 Transportation Security Enforcement Record System

Background: This system of records allows DHS/TSA to collect and maintain records related to the TSA's screening of passengers and property, as well as records related to the investigation or enforcement of transportation security laws, regulations, directives, or federal, state, local, or international law.

Purpose: The purpose of this system is to maintain an enforcement and inspections system for all modes of transportation for which TSA has security-related duties and to maintain records related to the investigation or prosecution of violations or potential violations of federal, state, local, or international criminal law. Records may be used to identify, review, analyze, investigate, and prosecute violations or potential violations of transportation security laws, regulations, and directives or other laws; they can also identify and address potential threats to transportation security and record the details of TSA security-related activity, such as passenger or property screening. TSA updated this SORN to cover records relating to the TSA Internet Transfer Protocol, to modify the category of individuals and category of records, to reflect an approved records retention schedule for records covered by this system, and to modify two existing routine uses. *(August 28, 2018; 83 FR 43888))*

4. DHS/USCG-008 Courts-Martial and Military Justice Case Files System

Background: This system of records allows the United States Coast Guard (USCG) to collect and maintain records regarding military justice administration and documentation of USCG Courts-Martial proceedings.

Purpose: The purpose of this system is to document military justice administration and documentation of USCG Courts-Martial proceedings relating to all USCG active duty, reserve, and retired active duty and retired reserve military personnel and other individuals who are tried by, or involved with, court martial. *(May 9, 2019; 84 FR 20383))*

Computer Matching Agreements

Under the *Computer Matching and Privacy Protection Act of 1988*, that amended the Privacy Act, federal agencies must establish a Data Integrity Board to oversee and approve their use of Computer Matching Agreements (CMA).[14] The CPO serves as the Chairperson of the DHS Data Integrity Board (DIB), and members include the Inspector General, the Officer for CRCL, the CIO, and representatives of Components that currently have an active CMA in place.[15]

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 a written CMA with the other party, which must be approved by the DIB. CMAs are required when there is a comparison of two or more automated systems of records for verifying the eligibility for cash or in-kind federal benefits.[16]

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

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

The DIB conducted its annual review of CMA activity and submitted the Department's *Computer Matching Activity Annual Report* to OMB, covering Calendar Year 2018.

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

[14] 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).

[15] 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).

[16] 5 U.S.C. § 552a(o).

Privacy Oversight

Privacy Compliance Reviews

The Privacy Office exercises its oversight function under Section 222 of the Homeland Security Act to ensure the Department's use of technology sustains, and does not erode, privacy protections,[17] primarily by conducting PCRs.[18] PCRs are a *constructive and collaborative* mechanism to assess implementation of protections described in PIAs, SORNs, or ISAAs; to identify areas for improvement; and to correct course if necessary. PCRs are distinct from the CPO's investigative authority.

The PCR framework emphasizes program involvement throughout the process to build trust with affected systems or programs. 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 affected programs, the Privacy Office, and Component Privacy Officers.

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

During the reporting period, the Privacy Office completed three PCRs, oversaw implementation of recommendations from six previous PCRs, and launched two new PCRs.

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

PCRs Completed

Section 1367 Privacy Incidents, February 2019[19]

The Privacy Office conducted a PCR to assist certain Components to identify and mitigate risks that may occur by inadvertent disclosure of information protected by Title 8, United States Code (U.S.C.), Section 1367, confidentiality and prohibited source provisions. Section 1367 incidents are particularly sensitive given the vulnerability of the population they are meant to protect and

[17] 6 U.S.C. § 142(a)(1).

[18] DHS Instruction 047-01-004 for Privacy Compliance Reviews, *available at*: https://www.dhs.gov/publication/dhs-privacy-policy-instruction-047-01-004-privacy-compliance-reviews.

[19] *Available at*: https://www.dhs.gov/sites/default/files/publications/1367%20PCR%20Report%20FINAL%2020190204.pdf.

the potential legal liabilities for certain violations of the statute. Through this PCR, the Privacy Office examined the Components' privacy protections and made four best practice recommendations to prevent and mitigate future privacy incidents affecting individuals protected by Section 1367.

Countering Violent Extremism Grant Program (CVEGP), April 2019[20]
Beginning in 2016, the former DHS Office of Community Partnerships and FEMA managed the CVEGP to fulfill a congressional mandate to help states and local communities prepare for, prevent, and respond to emergent threats from violent extremism. The CVEGP PIA[21] discussed the privacy risks of the first iteration of this grant program. The PIA noted that the Privacy Office would initiate a PCR to provide recommendations for improving the privacy protections inherent in deploying a security review process as part of the grant application process.

While the CVEGP was not renewed after its initial 2016 funding, the findings and three recommendations reflected in this report serve as lessons learned that the newly formed Office of Terrorism Prevention Partnerships and the Office for Targeted Violence and Terrorism Prevention should carefully consider for any future CVEGP iterations, if applicable. Further, the PCR advised the FEMA Grant Programs Directorate, as the administrator and manager of DHS grants, to fully implement the Privacy Office's recommendations to improve privacy protections for any future grant program that includes a security review.

DHS Science and Technology Directorate, June 2019[22]
The Privacy Office conducted a PCR because of growing concerns that DHS S&T's privacy compliance process, particularly for those programs involving social media and volunteers, did not meet requirements under DHS policies. Findings detailed in the PCR report reflect conclusions reached based on the Privacy Office's historical interactions with the DHS S&T Privacy Office, as well as an analysis of documents, responses, discussions, and other information received from the DHS S&T Privacy Office over the course of our review. The six recommendations promote the best practices of a well-functioning privacy program.

PCRs Continued Oversight

Office of the Chief Human Capital Officer, September 2015 with ongoing oversight[23]
The Privacy Office completed a PCR of the Office of the Chief Human Capital Officer (OCHCO) in 2015 that included 25 recommendations to improve the culture of privacy at OCHCO. The recommendations focused on the areas of transparency/raising awareness, data minimization/retention limits, use limitations, data integrity, data security, and accountability.

Since publishing the 2015 PCR findings, the Privacy Office has met with the Chief Human Capital Officer and OCHCO staff on multiple occasions to encourage implementing the recommendations, focusing on how OCHCO will make sustainable plans and actions to change the culture within the office. OCHCO submitted implementation status reports to the DHS

[20] *Available at*: https://www.dhs.gov/publication/countering-violent-extremism-grant-program-0.
[21] *Available at*: https://www.dhs.gov/publication/dhsallpia-057-countering-violent-extremism-grant-program.
[22] *Available at*: https://www.dhs.gov/publication/pcr-s-t-directorate
[23] *Available at*: https://www.dhs.gov/publication/privacy-compliance-review-office-chief-human-capital-officer.

Privacy Office in September 2016, April and September 2017, and June 2018, in compliance with the 2015 PCR self-audit requirement.

In February 2019, the Privacy Office determined OCHCO satisfactorily implemented all 2015 PCR recommendations, specifically noting that OCHCO's new privacy team, SOPs, and Privacy Action Plan were key to implementation. The Privacy Office did note, however, that some recommendations hinge on sustaining compliance, oversight, and relevance of OCHCO's Privacy SOP, and the Privacy Office further expanded two recommendations to address training needed to mitigate privacy incidents.

Analytical Framework for Intelligence, December 2016 with ongoing oversight [24]
CBP 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, the Privacy Office conducted a PCR to assess adherence to the privacy protections articulated in its privacy compliance documentation. 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 second PCR was published on December 6, 2016, with eight additional recommendations to improve its ability to demonstrate compliance with privacy requirements.

In October 2017, the Privacy Office noted CBP's responsible stewardship and privacy oversight of AFI and the implementation of most PCR recommendations. At that time, three PCR recommendations required continued oversight and CBP was asked to provide an implementation update within six months. In February 2019, the Privacy Office determined CBP had satisfactorily implemented all the PCR recommendations.

Nationwide Suspicious Activity Reporting (SAR) Initiative, April 2017 with ongoing oversight[25]
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, which is held in the FBI's eGuardian system. "Suspicious activities" is 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 eGuardian as Information Sharing Environment-Suspicious Activity Reports (ISE-SAR).

The November 2010 DHS ISE-SAR Initiative PIA and subsequent May 2015 update[26] identified and assessed the privacy risks associated with DHS Components' participation in the NSI. One

[24] *Available at*: https://www.dhs.gov/publication/privacy-compliance-review-analytical-framework-intelligence.
[25] This PCR is not posted on the DHS website.
[26] *Available at*: https://www.dhs.gov/publication/dhs-information-sharing-environment-suspicious-activity-reporting-initiative.

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 ISE-SARs. To reduce this risk, the 2010 PIA required the Privacy Office to conduct a PCR.

An initial PCR, completed in October 2012, resulted in five recommendations crafted to help ensure privacy rights, 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 SAR Initiative Management Group, and both initial and refresher training regimens.

The Privacy Office launched a follow-up to the 2012 PCR in October 2015 to assess whether Components had implemented the five recommendations from the 2012 PCR. The Privacy Office 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. The Privacy Office finalized its second NSI PCR in April 2017, which resulted in seven additional recommendations. The Privacy Office met individually with each Component to discuss the impetus for the PCR, its methodology, how the Privacy Office reached its conclusions, and what each specific privacy office could do to improve its Component's compliance with both NSI and privacy requirements.

Throughout 2017 and 2018, the Privacy Office continued to seek updates from participating Components on their NSI activities and the implementation of the PCR recommendations. On May 20, 2019, the Privacy Office tasked the affected Components with two additional recommendations to improve privacy compliance.

USSS, July 2017 with ongoing oversight[27]
The Privacy Office launched a PCR on December 2, 2016, based on the DHS OIG recommendation[28] to "conduct a systemic review with recommendations for ensuring USSS compliance with DHS privacy requirements." The Privacy Office identified twelve recommendations designed to improve the culture of privacy at USSS, as well as the effectiveness of the USSS Privacy Office.

USSS provided the Privacy Office with status updates in August 2018 and February 2019, demonstrating steps taken to implement the PCR recommendations. While positive steps have been taken to improve USSS compliance with DHS privacy requirements, the PCR recommendations have not been fully implemented.

USCIS National Appointment Scheduling System and Customer Profile Management Service, October 2017 with ongoing oversight[29]

[27] *Available at*: https://www.dhs.gov/publication/privacy-compliance-review-us-secret-service-usss.
[28] *See* OIG-17-01 report, "USSS Faces Challenges Protecting Sensitive Case Management Systems and Data", October 7, 2016.
[29] *Available at*: https://www.dhs.gov/publication/privacy-compliance-review-uscis-customer-profile-management-service-and-national.

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 the National Appointment Scheduling System (NASS). Due to the heightened privacy risks associated with the collection of biometrics, PIAs[30] for CPMS and NASS in 2015 required the Privacy Office to conduct a PCR. The Privacy Office identified six recommendations designed to improve USCIS privacy compliance, and to incorporate best practices for other USCIS and DHS programs and systems.

In April 2019, the Privacy Office determined USCIS adequately addressed all six recommendations but encouraged USCIS to promote best practice recommendations as appropriate and continue to ensure compliance with its retention schedule.

Media Monitoring Capability, December 2017 with ongoing oversight[31]
The Privacy Office launched its eighth PCR of the Office of Operations Coordination (OPS) National Operations Center (NOC) Media Monitoring Capability (MMC) on June 26, 2017, to determine whether the MMC's collection and use of social media information complies with the privacy mitigations described in its PIA,[32] as well as its implementation of recommendations from previous PCRs. While the Privacy Office found that OPS NOC MMC is an outstanding example of an office with a healthy privacy culture with a commitment to protect individuals' privacy, the Privacy Office made five recommendations to better comply with DHS policies. As of May 2019, OPS partially implemented three recommendations and fully implemented two recommendations.

PCRs Launched

- *Center of International Safety and Security's Foreign Access Management System* (FAMS), April 2019. The primary objective of this PCR is to determine whether the FAMS program was conducted in compliance with the associated PIA[33] and SORN.[34] This broad review is being conducted because of a privacy incident in which DHS PII was involved in a ransomware attack on the systems utilized by the FAMS Pilot.

- *FEMA Information Sharing Review*, April 2019. The DHS Privacy Office launched a PCR in response to FEMA's information sharing and oversight practices, particularly as they relate to compliance with departmental and internal FEMA guidance to ensure

[30] *See* DHS/USCIS/PIA-060 Customer Profile Management Service, *available at*: https://www.dhs.gov/publication/dhsuscispia-060-customer-profile-management-service-cpms, and DHS/USCIS/PIA-057 National Appointment Scheduling System, *available at*: https://www.dhs.gov/publication/dhsuscispia-057-national-appointment-scheduling-system.
[31] *Available at*: https://www.dhs.gov/publication/privacy-compliance-reviews-media-monitoring-initiative.
[32] *See* DHS/OPS/PIA-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative, *available at*: https://www.dhs.gov/publication/dhs-ops-pia-004f-publicly-available-social-media-monitoring-and-situational-awareness.
[33] *See* DHS/ALL/PIA-048(b) Foreign Access Management System (FAMS), *available at:* https://www.dhs.gov/sites/default/files/publications/privacy-pia-all048-fams-april2017.pdf.
[34] *See* DHS/ALL-039 Foreign Access Management System of Records, May 1, 2018, *available at:* https://www.federalregister.gov/documents/2018/05/01/2018-09196/privacy-act-of-1974-system-of-records.

information sharing and safeguarding activities associated with two FY19 privacy incidents.

***Figure 3*: Implementation Status of All PCR Recommendations (as of June 30, 2019)**

PCR Name (Component)	Date published	Total Number of Recommendations	Recommendation Implemented (#)	Implementation in progress (#)	Recommendation not implemented (#)
Enhanced Cybersecurity Services (CISA)	4/10/15	4	4		
Office of the Chief Human Capital Officer (OCHCO)	9/30/15	23	23		
Analytical Framework for Intelligence (CBP)	12/6/16	8	8		
Southwest Border Pedestrian Exit Field Test (CBP)	12/30/16	10	10		
USSS	7/21/17	12	3	9	
Customer Profile Management Service & National Appointment Scheduling System (USCIS)	10/11/17	6	5	1	
Electronic System for Travel Authorization (CBP)	10/27/17	3	1		2* *Implementation hinges on mandatory submission of social media information
Publicly Available Social Media Monitoring and Situational Awareness Initiative (OPS)	12/8/17	5	2	3	
Privacy Incidents Affecting Individuals Protected by Section 1367 (Multiple)	2/4/19	4		4	
Countering Violent Extremism Grant Program (FEMA)	4/12/19	3		3	
DHS Science and Technology Directorate	6/24/19	6		6	

Privacy Incidents

The Privacy Office manages privacy incident response for the Department. DHS 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 ESOC, Component SOCs, Component Privacy Officers and PPOCs, and DHS management officials.

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

- hosting a monthly Department-wide Incident Practitioner meeting to identity and discuss trends, problem-solve, and share incident response and mitigation best practices;
- analyzing incident trends and trouble-shooting incident causes to promote prevention efforts;
- identifying vulnerabilities in data handling practices and reaching out to specific Components for refresher trainings (i.e., at new employee orientations, town halls, participating in "Privacy Day");
- sending periodic email messages to encourage all staff to report privacy incidents immediately and conveying best practices to prevent an incident;
- working with the HQ IT Service Desk to create a new online portal to make it easier for staff to report privacy incidents. As a result, there has been an increase in employees contacting the Privacy Office to discuss suspected incidents;
- partnering with the SOC's Risk Management Division to perform system security scans and directory folder sweeps to keep file data secure and dispense guidance regarding storing PII on shared drives;
- participating in the Federal Privacy Council's Federal Breach Response and Identity Theft Subcommittee to share best practices with other federal agencies; and
- establishing a closer working relationship with the DHS Security Operations Team as part of the Privacy Office holistic view of incident handling. Both sides have learned from each other and are more effective when remediating daily incidents as a team.

Incident Policies

The Privacy Office authored the *DHS Privacy Incident Handling Guidance* (PIHG), the foundation of DHS privacy incident response. DHS defines a privacy incident[35] as 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.

Second Annual Privacy Incident Tabletop Exercise

On April 16, 2019, the Privacy Office sponsored the second annual DHS Privacy Incident Tabletop Exercise in Washington, DC. The exercise was conducted jointly with the Component SOCs, led by the ESOC management team. FEMA's National Exercise Division facilitated the exercise, with privacy representatives from all DHS Components in attendance.

The goal of this annual exercise is to refine and validate the breach response plan in the PIHG and the Major Cybersecurity Incident Response Guide through a simulation and identify any potential gaps or weaknesses in the breach response process at both the Component and enterprise levels.

This past year, Components were encouraged to conduct their own tabletop exercises and asked to invite the Privacy Office as an observer. CISA conducted a successful exercise on September 18, 2018. USCIS is in the process of planning their own tabletop exercise as well.

Incident Metrics

When a privacy incident is reported, the CPO, in consultation with the Component Privacy Officer and other appropriate parties, must determine if the incident is a minor or major incident based on the context, evaluating the 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; the CPO may delegate this responsibility to the affected Component.

During this reporting period, 952 total privacy incidents were reported to the DHS SOC. Figure 4 shows the total broken down by Component. From this total, PRIV deducted 83 incidents involving multiple Components, along with 12 incidents that were determined to be non-incidents, for a net total of 857 privacy incidents. There were 95 more incidents reported this year compared to last, an increase of 11%. This increase may be an indicator that Privacy Office training and outreach programs are working.

[35] 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. The Privacy Office kept the term "privacy incident" to be consistent with other DHS incident types.

Figure 4: Total number of privacy incidents
by DHS Component for the period July 1, 2018 – June 30. 2019

Component	Privacy Incidents
CBP	54
CISA	22
FEMA	42
FLETC	3
HQ	14
ICE	75
OIG	3
S&T	1
TSA	20
USCG	64
USCIS	641
USSS	13
Total	**952**

Major Incidents: FEMA and CBP

Major Incident Involving FEMA's Transitional Shelter Assistance Program

On November 9, 2018, the OIG issued a draft of its *Management Alert: FEMA Did Not Safeguard Disaster Survivors' Sensitive Personally Identifiable Information*. The alert noted that FEMA provided more PII to a contractor than was required for the contractor to carry out its contract services to meet temporary shelter needs of disaster survivors. This data included survivor banking information that was necessary to carry out an earlier iteration of the Transitional Shelter Assistance (TSA) program but was no longer necessary. OIG determined that approximately 2.5 million survivors of hurricanes Harvey, Irma, and Maria, as well as the California Wildfires of 2017, were impacted.

Upon investigation of the matter, FEMA confirmed OIG's findings that FEMA shared banking and home address information with the contractor that FEMA determined to be more than necessary for the contractor to administer the TSA program. A previous iteration of the TSA program, known as TSA-Reimbursable Program (TSAR), required the provision of additional information to the contractor, including banking information. However, TSAR has not been utilized by FEMA since 2008 and was not utilized during the aforementioned disasters. Since the initial assessment, FEMA found that roughly 2.5 million disaster victims' Sensitive PII and PII were impacted.

Based on the advice of the Breach Response Team, led by the CPO, the Acting Secretary approved notification and credit monitoring services for all 2.5 million effected disaster survivors.

Since discovery of this issue, FEMA has taken measures to correct this error. FEMA is no longer sharing unauthorized data with the contractor and has conducted a detailed review of the contractor's information system. FEMA has also worked with the contractor to remove the unauthorized data from its system.

Major Incident Involving FEMA Information Sharing
On January 11, 2019, the FEMA Texas Recovery Office notified FEMA Headquarters of potential unauthorized sharing of disaster survivors' PII with a non-governmental disaster relief organization. This organization is an association of national, state, and territory member organizations that mitigate and alleviate the impact of disasters. The organization provides disaster case management (DCM) services for individual disaster survivors. In this role, they coordinate with 13 other non-profit member organizations to offer survivors services or other unmet disaster caused needs. To perform the DCM services, the organization is authorized to receive limited survivor PII in order to contact them and offer appropriate, relevant services.

Initially, FEMA identified an ISAA executed between FEMA and the organization related to FEMA's response efforts to Hurricane Harvey. This ISAA enabled FEMA to leverage the appropriate organization membership and served as a force multiplier in supporting survivors. The ISAA permitted FEMA to share name and contact information with the disaster relief organization. However, FEMA discovered additional data elements were also shared, including birthdates, FEMA registration identification numbers (FEMA Reg ID), and other information related to the type of FEMA assistance provided. This information shared was connected to approximately 895,000 survivors.

Further investigation found a FEMA-State Agreement (FSA) between FEMA and the State of Texas. This FSA was amended with the intent to authorize the organization to perform DCM services in support of survivors. By amending the FSA, FEMA identified this organization as having a legitimate business justification to receive the additional PII, and the ISAA was neither required nor controlling. Therefore, FEMA initially concluded that the sharing of such PII data with the organization was and is authorized, but the amended FSA lacked the appropriate specifics and was not entirely consistent for this type of sharing with this organization and additional non-profit member organizations.

To mitigate this incident, FEMA amended the FSA on February 7, 2019, to further clarify that the disaster relief organization should have the same level of access to data as the State and includes the specific non-profit member organizations that receive FEMA data through this organization's onward sharing. Additionally, the original ISAA that was executed in error was terminated, as it was deemed unnecessary given the FSA amendments.

Major Incident Involving CBP License Plate Reader Pilot
In late May, the CBP SOC discovered media reports about a ransomware attack on a CBP subcontractor that specifically identified CBP data. In response to CBP inquiries, the CBP primary contractor notified CBP that its subcontractor took unauthorized copies of CBP PII and copied it onto its own corporate servers. In turn, CBP independently confirmed this report through its own direct investigation into the matter.

While the investigation is ongoing, preliminary evidence indicates several violations of CBP privacy and security policies and specific contract clauses. In response, CBP has taken the following actions:

- Issued a letter to the prime contractor, demanding a series of remediation steps, including requiring a detailed list of risk mitigation/management controls that the primary contractor intends to perform, preserving all data regarding the ongoing investigation, confirmation of specific facts regarding the incident, and other matters. The letter also stated that CBP finds it wholly unacceptable that a subcontractor appears to have violated security and privacy protocols.
- Required the prime contractor to immediately terminate its subcontracting arrangement with the subcontractor in question. This subcontractor no longer has access to CBP data and is in the process of returning all government equipment in its possession. Further, to date, CBP has removed from service all equipment related to this specific breach.

The subcontractor violated mandatory security and privacy protocols outlined in its contract. None of the CBP image data was identified as having been further disclosed because of the cyber-attack against the subcontractor's network. CBP is working closely with law enforcement and cybersecurity entities, and its own Office of Professional Responsibility to investigate the incident. DHS and CBP continue to work with all partners to determine the extent of the major incident/breach, as well as the appropriate mitigation and remediation actions.

Special Protected Classes – Unauthorized Disclosures

Confidentiality protections afforded to alien victims of crimes are statutorily required under Title 8, United States Code, Section 1367, *Violence Against Women Act* (herein Section 1367), as well as T and U visa applicants. The Officer for CRCL has, through Secretarial delegation, the authority to provide DHS-wide guidance and oversight on the implementation of Section 1367 confidentiality and prohibited source provisions. The CPO must determine any potential impact a privacy incident may have on the privacy of individuals, including those protected by Section 1367.

Because of shared responsibilities for ensuring the proper handling of Section 1367 information, in FY 2018 the Privacy Office and CRCL developed a process whereby two offices share incidents of unauthorized Section 1367 disclosures. The Privacy Office collaborated with the Department's Enterprise Cyber Operations Portal (ECOP) developers to add specific Special Protected Class (SPC) checklist questions to the privacy incident reporting process to prompt analysts that may work with SPC data and to assist with overall SPC incident tracking. The two offices then work together to ensure all incidents are appropriately investigated, addressed, and resolved.

During this reporting period, the Privacy Office hosted two SPC Unauthorized Disclosure forums to refresh and educate the PPOCs and Incident Practitioners. Section 1367 incident reporting has increased, which is a positive indicator that the Department-wide outreach is taking effect. Of the 850 total confirmed privacy incidents during this reporting period, there have been 51 SPC-related incidents reported: 35 confirmed; 14 suspected; and 2 investigated and found not related to SPC.

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*,[36] 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, when available.[37] U.S. citizens, Lawful Permanent Residents (LPR), visitors to the United States, and aliens may submit privacy complaints to the Department.[38] The Privacy Office also reviews and responds to privacy complaints referred by employees throughout the Department or those submitted by other government agencies, the private sector, or the public. DHS Components manage and customize their privacy complaint handling processes to align with their specific missions and to comply with Department complaint handling and reporting requirements.

DHS separates privacy complaints into four types:

1. ***Procedure:*** Issues concerning process and procedure, such as consent, collection, and appropriate notice at the time of collection, or notices provided in the *Federal Register,* such as Privacy Act SORNs.
    a. *Example*: An individual alleges that a program violates privacy by collecting SSNs without providing proper notice.
2. ***Redress:*** Issues concerning appropriate access (not to include FOIA or Privacy Act requests) or correction to PII held by DHS. Also includes DHS TRIP privacy-related complaints. See below for more information.
    a. Example: Misidentification during a credentialing process or during traveler inspection at the border or screening at airports.
3. ***Operational:*** Issues related to general privacy concerns or other concerns that are not addressed in process or redress but don't pertain to Privacy Act matters.
    a. *Example:* An employee's health information was disclosed to a non-supervisor.
    b. *Example:* Physical screening and pat down procedures at airports.
4. ***Referred*:** Complaints referred to another federal agency or external entity for handling.
    a. *Example:* An individual submits an inquiry regarding his driver's license or SSN.

[36] 42 U.S.C. § 2000ee-1(f).

[37] These semi-annual reports may be found here: https://www.dhs.gov/publication/dhs-section-803-reports-congress/.

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

In addition, the Privacy Office reviews redress complaints received by the DHS Traveler Redress Inquiry Program (DHS TRIP) that may have a privacy nexus. DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs - like airports - or crossing U.S. borders. This includes watch list issues, screening problems at ports of entry, and situations where travelers believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at our nation's transportation hubs.

The DHS TRIP complaint form includes a privacy check box that reads: *I believe my privacy has been violated because a government agent has exposed or inappropriately shared my personal information.* From October 1, 2018 – June 30, 2019, PRIV received 558 such complaints. Of the 558 complaints, only one fit the privacy-nexus criteria (sent to ICE Privacy – loss of control). However, six other complaints were forwarded for further review (based on the nature of the complaint): two were sent to CRCL regarding traveler care, and four were sent to CBP regarding data integrity.

Between April 1, 2018 and March 31, 2019, the Department received 12,164 privacy complaints. In October 2019, the DHS Privacy Office began reporting complaints by type and Component, hence the need for the two charts below.

Figure 5: Privacy Complaints Received by DHS
April 1, 2018 – March 31, 2019

Privacy Complaints Received by DHS Components and TRIP: *April 1 – September 30, 2018*										
Type	**CBP**	**CISA**	**FEMA**	**ICE**	**TSA**	**USCG**	**USCIS**	**USSS**	**TRIP**	**ALL**
Procedure										736
Redress										5,153
Operational										2,681
Referred										439
TOTALS										**9,009**

Privacy Complaints Received by DHS Components and TRIP: *October 1, 2018 – March 31, 2019*[39]										
Type	**CBP**	**CISA**	**FEMA**	**ICE**	**TSA**	**USCG**	**USCIS**	**USSS**	**TRIP**	**ALL**
Procedure	422	0	0	0	9	0	0	0		431
Redress	59	0	0	0	0	0	0	0	7	66
Operational	2,406	0	0	0	141	0	0	0		2,547
Referred	111	0	0	0	0	0	0	0		111
TOTALS	**2,998**	**0**	**0**	**0**	**150**	**0**	**0**	**0**	**7**	**3,155**

[39] For efficiency, the data reflects the reporting period used in the Section 803 Reports.

Privacy Act Amendment Requests

The *Privacy Act* permits an individual, as defined by the *Privacy Act* as a U.S. citizen or LPR, or defined as a covered person by the *Judicial Redress Act of 2015*, to request amendment of his or her own records.[40] 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 6: Privacy Act Amendment Requests received by DHS during the reporting period by Component and disposition.

Privacy Act Amendment Requests July 2018 – June 2019				
Component	**Received**	**Granted**	**Denied**	**Pending**
CBP	10	1	1	8
FLETC	1	1	0	0
ICE[41]	8	1	7	0
OBIM	3	2	0	1
TSA	4	0	2	2
USCIS	5	0	1	4
TOTALS	**31**	**5**	**11**	**15**

Non-Privacy Act Redress Programs

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

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 information in its systems.

- OBIM responded to 133 redress requests during the reporting period.

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

[40] 5 U.S.C. § 552a(d)(2).
[41] ICE received a total of 10 Privacy Act amendment requests, but two were deferred to other agencies. This table only reflects the requests processed by ICE.

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 6,812 appeals and denied 623.
- Additionally, OIA granted 2,040 waivers and denied 329.

Information Sharing and Intelligence Activities

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

The work of the Privacy Office supports all six 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)

The DARC is the coordinated oversight and compliance mechanism for 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 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. As a discretionary matter, the DARC may also review any matter referred by a member concerning the internal or external transfer of data or the development, execution, implementation, or operation of any departmental information system with the concurrence of other members.

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

During the reporting period, the Privacy Office worked with DHS stakeholders and IC partners to approve ten ISAAs or extensions for existing arrangements and to 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.

Intelligence Product Reviews

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

The Privacy Office's product review function is an ongoing, real-time operational service for the Department, requiring round-the-clock monitoring of communications and quick response to I&A's requests for review of intelligence products. During this reporting period, the Privacy Office reviewed 251 IIRs and FINTEL, 17 briefing packages, and 267 RFI (at all levels of classification). The Privacy Office also reviewed I&A's standing information requirements to ensure that DHS did not solicit unauthorized or unneeded PII.

The Privacy Office, in cooperation with OGC's Intelligence Law Division, I&A's Intelligence Oversight Officer, and CRCL, is working closely with I&A to change the process from one of pre-publication review to post-production audit for FINTEL and IIRs. During the current reporting period, the Privacy Office and its partner offices audited a random sample of IIRs produced by a Component that routinely publishes a high volume. This audit was intended to test the four offices' ability to conduct an audit where the Component is prolific. The offices involved are reviewing audit procedures with the intent of implementing IIR audits on a larger scale and with greater frequency, without requiring additional resources.

Mission Number One: Prevent Terrorism and Enhance Security.

III. Privacy Best Practices

The Privacy Office's FY 2019-2022 Strategic Plan includes:

***Goal Three*: Integrate privacy best practices into Department operations and processes.**

The Privacy Office strives to create and implement best practices while achieving strategic goals and objectives. Specific examples for each strategic objective are detailed below.

Objective 3.1: Improve collaboration with key stakeholders to align privacy processes with operational needs.

- **Screening and Vetting Initiatives**: As explained in Part Two, the Privacy Office is directly engaged in oversight and governance efforts related to NSPM-9 and the on-going activities of the NVC. The P-CRCL Working Group, comprised of senior privacy and civil liberties officials from several departments and agencies supporting the implementation of NSPM-9, ensures that the activities of the NVC Governance Board and NVC appropriately protect individuals' privacy, civil rights, and civil liberties. It also provides specific advice and guidance to the NVC and the Governance Board on privacy and civil liberties issues. Privacy Office staff are members of the Working Group, which meets regularly to evaluate screening and vetting program proposals, the attendant Implementation Plans, Concepts of Operations, and technology structures within a FIPPs-based risk assessment model. To further support privacy oversight and governance, the NVC staffed a P-CRCL Officer, reporting to the P-CRCL Co-Chairs, who is charged

with incorporating privacy, civil rights, and civil liberties into all aspects of planning and implementation for the NVC.

Objective 3.2: Increase compliance by developing trust and building partnerships with operators and program offices to integrate privacy into program and technology planning, design, and deployment.

- **New SSN Reduction Initiative**: The new privacy policy will require new and existing IT systems to either adopt an alternative identifier or to mask the SSN wherever it appears. With over 700 DHS systems currently collecting and/or using the SSN, this multi-year initiative will involve:
    1. training privacy staff and IT program managers on how to implement the policy requirements;
    2. working with CHCO's new Data Governance Council to encourage human capital IT system program managers across DHS to adopt the alternative identifier;
    3. collaborating with agency partners to perfect another alternative identifier that can be implemented in non-human capital systems;
    4. partnering with the CISO Council to test a new alternative identifier; and
    5. working with program managers of IT systems that cannot adopt an alternative identifier to re-code their systems to mask or truncate the SSN.

Objectives 3.3: Develop and implement compliance, governance, and oversight models for Department pilots, programs, and information sharing initiatives.

- **Insider Threat Program**: As explained in Part Two, Privacy Office staff play a central role on the 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, CRCL, and the Privacy Office. The ITOG meets quarterly to review quarterly reports that provide anonymized details of all ITP activities and investigations and makes recommendations for new policies or procedures based on its review of the quarterly reports. The ITOG also meets as needed to discuss new user activity monitoring policies and to authorize enhanced user activity monitoring of individuals who appear to pose an insider threat to DHS. Privacy Office staff are also working with the other members of the ITOG to finalize auditing procedures.

- **Trusted Identity Exchange (TIE):** TIE is a privacy-enhancing DHS Enterprise Service that enables and manages the digital flow of identity, credential, and access-management data for DHS personnel. It does so by establishing connections to various internal authoritative data sources and providing a secure, digital interface to other internal DHS consuming applications. A consuming application is any DHS system that requires some form of identity, credential, and access-management data in order to grant logical or physical access to a DHS protected resource. The Privacy Office meets weekly with the TIE team to discuss and analyze the privacy implications, risks, and requirements of new sharing with consuming applications. Additionally, each attribute consumer provides the business case for the attributes requested from authoritative data sources that must be approved by the Privacy Office. This relationship with the TIE team ensures that (1) compliance requirements are completed at the appropriate time; (2) governance

requirements related to data access are properly implemented; and (3) oversight of data sharing is effectively administered.

IV. FOIA Operations

The Privacy Office's FY 2019-2022 Strategic Plan includes:

***Goal Four (FOIA Compliance)*: Provide timely disclosures pursuant to the FOIA, improve responsiveness, and reduce the number and age of pending open FOIA requests.**

The Privacy Office, led by the CPO (who is also the Chief FOIA Officer), is responsible for FOIA policy, program oversight, training, and the efficacy of the DHS FOIA program. Privacy Office leadership meets regularly with DHS leadership to ensure the Department continues to emphasize processing FOIA requests, backlog reduction, closing the agency's ten oldest requests, consultations and appeals, FOIA training, and that the DHS Component FOIA offices have the resources required to keep the FOIA programs running efficiently and providing a high level of customer service.

The Department's FOIA Program processes the largest volume of requests and has the second-largest staff in the Federal Government. In FY 2018, 579 FOIA personnel processed more than 374,946 requests—releasing more than 35 million pages of records.

For more detailed information, please consult the 2019 Chief FOIA Officer Report.

FOIA Compliance and Oversight

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

As part of this compliance review, the Chief FOIA Officer compiled and assessed responses to the DOJ Self-Assessment Tool-Kit from Component FOIA Officers. The Self-Assessment Tool-Kit is comprised of 13 modules on a variety of FOIA functions. From the responses, the Chief FOIA Officer identified shared challenges and opportunities to improve performance through the use of best practices. The Chief FOIA Officer builds on the baseline understanding of Component compliance issues that surfaced in the self-assessment responses by requiring Component FOIA Officers to periodically re-assess performance on certain modules and developing and conducting DHS-specific compliance assessments.

FOIA Operations:[42] DHS consistently receives the largest number of FOIA requests of any federal department or agency, more than 40 percent of all requests within the Federal Government. This year's increase tracks with the increased public interest in the Department's operations, including the execution of Departmental priorities like recent Presidential EOs and guidance from the Secretary. In FY 2018, DHS received an eight percent increase in requests from FY 2017 –from 366,036 to 395,751 – and processed a record-setting 374,945 requests – a two percent increase from FY 2017. The DHS FOIA Program released almost 35 million pages, including 140,000 pages through the appeals process and 300,000 pages in litigation.

FOIA Backlog: Despite processing a record-setting number of requests in FY 2018, the backlog increased due to the number of requests received. At the end of FY 2018, the backlog was 53,971 – a 22 percent increase over FY 2018. This increase occurred despite an aggressive effort by the Privacy Office to use its resources to assist Components in reducing their backlogs. The Privacy Office collaborated with CISA, CBP, and ICE to eliminate about 12,000 requests from the backlog prior to the end of the fiscal year. CISA decreased its backlog by 37 percent, despite receiving 37 percent more requests in FY 2018, and FEMA further decreased its backlog by 32 percent, successfully reducing the backlog from almost 1,500 requests to about 200 requests over two years.

Modernization and Consolidation of FOIA IT Efforts: As mentioned earlier in the report, the Privacy Office continued its work to modernize and consolidate FOIA IT systems across DHS. The Privacy Office built off the support from former Deputy Secretary Elaine Duke to make addressing outdated FOIA IT systems a budget and resource priority. The Privacy Office is also

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

utilizing the work of the enterprise-wide FOIA Technology System Requirements Working Group to address outdated and duplicative FOIA IT Systems throughout DHS.

The Privacy Office is in the procurement process to purchase a FOIA IT solution that makes powerful e-discovery and computer-assisted redaction technology available to FOIA processors at all Components that choose to use the solution. The solution will also allow requesters to electronically submit requests to the system and enable cases to be easily transferred between participating Components, eliminating a significant amount of administrative work. The seamless transfer of cases also allows participating Components to assist if there is a surge in FOIA requests or a need for concentrated backlog reduction efforts as in years past. The solution will also be interoperable with other processing solutions across the Department.

FOIA Policy

The Privacy Office made significant strides in developing and implementing policy to improve the administration of the FOIA and ensure consistency in its application throughout the Components:

- In May 2019, the Privacy Office issued Instruction 262-11-002, *Freedom of Information Act Reporting Requirements*,[43] to formalize and clarify roles and responsibilities in weekly, monthly, and annual reporting and in the one-day notification process for significant requests.
- In May 2019, the Privacy Office convened the initial meeting of the DHS FOIA Council.[44] The Council was chartered in November 2018 to discuss policy and management matters concerning the departmental FOIA Line of Business functions. The Council is also a forum for sharing FOIA best practices and coordinating cross-Component challenges and developing solutions. The Council created the following four committees to conduct its work: Backlog, DHS FOIA Employee Development, Policy, and Technology.

FOIA Training

The FOIA Improvement Act of 2016 requires the agency Chief FOIA Officer "offer training to agency staff regarding their FOIA responsibilities."[45] The Privacy Office and the Component FOIA Offices conduct internal staff training to standardize FOIA best practices across the Department, and to promote transparency and openness within DHS and among the requester community. In addition, the Privacy Office and the Component FOIA Offices serve on various panels outside the Department, enabling them to (1) standardize FOIA best practices across the Department and (2) promote transparency and openness within DHS and among the requester community.

[43] For information regarding this instruction and other DHS FOIA Regulations, Management Directives, and Instructions see https://www.dhs.gov/foia-statutes-resources.
[44] For information regarding the DHS FOIA Council Charter, dated November 7, 2018, see https://www.dhs.gov/publication/foia-council-charter.

[45] 5 U.S.C. § 552 (j)(2)(F).

The Chief FOIA Officer and the Deputy Chief FOIA Officer are members of the Chief FOIA Officer Council[46] 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 to increase transparency.

Privacy Office and Component FOIA training and awareness activities are detailed in the annual *Chief Freedom of Information Act Officer Report to the Attorney General of the United States,*[47] also available on our website.

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.

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

- Collaborated with the Department of the Treasury (Treasury) to host the 2019 Sunshine Week FOIA Training Summit. The Summit included one day of DHS-specific training and one day of joint training with Treasury and featured a keynote address from the Chief Judge of the District Court of the District of Columbia and the presentation of Sunshine Awards recognizing exceptional DHS FOIA employees.
- Partnered with OGIS to train DHS FOIA Professionals on Dispute Resolution Skills.
- Provided Advanced FOIA Training and Litigation Training for DHS FOIA professionals with at least one year of experience.
- Trained staff on issues with requests for contracts, fees and fee estimates, redacting records in litigation, segregating records, the foreseeable harm standard, the White House consultation process, Exemption 5 privileges, and standards for qualifying as a new media requester.

[46] 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.

[47] The DHS Chief FOIA Reports are available here https://www.dhs.gov/dhs-chief-foia-officer-reports.

V. Outreach, Education, and Reporting

The Privacy Office's FY 2019-2022 Strategic Plan includes:

Goal 5 *(Outreach, Education, and Reporting)*: Engage with internal and external stakeholders through training, education, and outreach to strengthen privacy and disclosure activities.

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

Outreach

Conferences and Events

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

- ***American Society of Access Professionals Eleventh National Training Conference***: In July 2018, in Arlington, VA, the CPO spoke on how DHS is improving FOIA responsiveness and performance to meet increasing demand, and the Deputy CPO, along with the Department of Transportation's CPO, co-presented scenario-based privacy challenges.
- ***Counter Unmanned Aircraft Summit***: August 22-24, 2018, Privacy Office staff provided an overview of the privacy issues related to the use of CUAS.
- ***Chief FOIA Officers Council Meeting***: July 19, 2018, in Washington, DC, the CPO spoke on how DHS has overcome challenges in FOIA administration and capitalized on new opportunities.
- ***Certified InfoSec Conference***: October 10, 2018, the CPO delivered the keynote address for the data privacy track entitled: *Where Are We in the American Privacy Movement?*
- ***National Defense Industrial Association Meeting***: October 17, 2018, the former CPO presented on *Privacy Programs and the General Data Protection Regulation.*
- ***Federal Privacy Summit:*** November 14, 2018, in Washington, DC, the Federal Privacy Council hosted its annual one-day workshop for government privacy professionals. The keynote speaker was LaTanya Sweeney, Ph.D., Harvard University.
- ***Integrated Air and Missile Defense Summit***: November 28-30, 2018, Privacy Office staff participated in two panels exploring the legal, privacy, and civil liberties aspects of the use of CUAS technologies.
- ***Countering Drones Global Summit***: December 10-13, 2018, in London, England, Privacy Office staff gave a presentation on the privacy aspects of the *Preventing Emerging Threats Act of 2018* to government officials from other countries who are exploring the acquisition of CUAS.
- ***Cybersecurity: Protecting Sensitive Information***: February 19, 2019, the CPO was a panelist at this workshop hosted by SheppardMullin.
- ***RSA Conference***: March 5, 2019, the CPO moderated a panel discussion: *Use of Facial Recognition to Combat Terrorism and Make International Travel More Secure.*
- ***Federal Privacy Council's Privacy Boot Camp***: March 11, 2019, the CPO gave a presentation entitled *Privacy 101: Privacy at a Federal Agency.*
- ***Sunshine Week:*** March 12-13, 2019, the DHS Privacy Office collaborated with Treasury to host the 2019 Sunshine Week FOIA Training Summit. The Summit included one day of DHS-specific training and one day of joint training with Treasury and featured a keynote address from the Chief Judge of the District Court of the District of Columbia and the presentation of Sunshine Awards recognizing exceptional DHS FOIA employees.
- ***International Association of Privacy Professionals (IAPP) Global Summit***: May 3-4, 2019, in Washington, DC, the CPO moderated two panel discussions: (1) *Use of Facial*

Recognition to Combat Terrorism and Make International Travel More Secure and (2) *Baking It In: Privacy Governance by Design in Large Organizations*.

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 SAOPs to share best practices, 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 Federal Privacy Council's committees and subcommittees and help plan its annual Federal Privacy Summit.

Data Privacy and Integrity Advisory Committee

The 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.[48] DPIAC members have broad expertise in privacy, security, and emerging technology, and they come from large and small companies, the academic community, and the non-profit sector. Members hold public meetings to receive updates from the Privacy Office on important privacy issues and to deliberate taskings from the CPO.

- On July 10, 2018, members of the DPIAC's Policy Subcommittee, along with officials from The Privacy Office and CBP's Offices of Privacy and Field Operations toured biometric entry and exit operations at Orlando International Airport to observe general passenger processing operations, including pilot entry and exit programs. Attendees were briefed on data collection, uses, and sharing associated with the entry processing of arriving visitors. They also received information on a pilot program in which CBP has collaborated with British Airways to use biometric data (facial images) to verify travelers' identity and process them for exit. The pilot utilizes an e-gate in the boarding area of the departure terminal and allows passengers to board their flight without

[48] 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.

presenting any travel documentation or a boarding pass. Back-end programming uses images captured at the gate to instantaneously match the individual to a gallery of previously captured images in order to verify their identity and match it to flight information. The CBP Privacy Office was able to verify that proper notification of the information collections, including signage, was in place and that travelers were made aware that participation in pilot activities was optional.

- On December 10, 2018, the DPIAC held a public meeting to review and discuss research findings regarding privacy considerations in biometric facial recognition technology. A follow up meeting by conference call was held on February 26, 2019, to finalize the DPIAC's recommendations report: *Privacy Recommendations in Connection with the Use of Facial Recognition Technology.*

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

Privacy and Civil Liberties Oversight Board

The Privacy Office participates in public and private meetings with the 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:

- **Machine Learning Working Group**: The PCLOB convened a Machine Learning Working Group focused on producing a framework that reflects inter-agency consensus on privacy and civil liberties principles to be used in machine learning development, acquisitions, and use in national security and law enforcement contexts. The Privacy Office is an active participant in these Working Group activities directed at helping reduce bias in machine learning training environments, producing a framework of principles to guide in the use of machine learning, and helping identify how to purge data without minimizing the utility of the respective algorithm.

- **Data Framework team:** This team had a status call with the PCLOB regarding issues that remained open as a part of the PCLOB's Oversight project on the Data Framework while the PCLOB was not operating with a quorum. During the call, the Data Framework team addressed the fact that many, if not all, of the issues that were previously under discussion were overtaken by events such as the discontinuance of Cerberus[49] (classified) functionality at the end of 2018, as well as the recasting of the Data Framework mission resulting from the passage of *The Data Framework Act of 2017*. PCLOB staff committed to deciding whether the line of query could be closed or should continue.

[49] https://www.dhs.gov/publication/dhs-all-pia-046-3b-cerberus

International Engagement & Outreach

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

During the reporting period, the Privacy Office met with 10 representatives from Austria, Belgium, Czech Republic, France, Germany, Ireland, and Poland. These engagements increased understanding of the U.S. privacy and FOIA frameworks, DHS privacy and disclosure policy, privacy compliance, information sharing, and incident response. By sharing DHS privacy compliance and policy practices with international partners and promoting the FIPPs, the Privacy Office conveys privacy best practices and builds the confidence necessary for cross-border information sharing and cooperation.

The Privacy Office keeps current on international developments by attending select international conferences. The CPO attended the Brussels portion of the 2018 International Data Protection and Privacy Commissioner's Conference in October. Privacy Office staff traveled to Vienna, Austria to attend the ID@Borders Conference, co-hosted by the Biometrics Institute and the Organization for Security and Cooperation in Europe.

The Privacy Office supports Department and U.S. government priorities by participating in interagency and international meetings, such as the US-Canada Executive Coordination Committee (ECC) meeting in June 2019. The ECC brought together principals from numerous federal government agencies in the United States and Canada to drive forward progress on cross-cutting bilateral issues, provide guidance, ensure accountability, and work collaboratively on shared agenda, priorities, and commitments. This year's ECC featured discussions on responsible expansion of information sharing initiatives.

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

Education: Privacy Training and Awareness

The Privacy Office develops and delivers a variety of ongoing and one-time privacy trainings 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 also detailed in the *Privacy Office Semi-Annual Reports to Congress,* 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 Training

DHS personnel attended instructor-led privacy training courses, including the following for which the Privacy Office either sponsored or provided a trainer:

- ***Fusion Center Training***: Privacy Office staff helped plan and deliver a Privacy and Civil Rights and Civil Liberties (P/CRCL) Workshop for fusion center privacy officers and senior personnel in Lincoln, Nebraska in the fall of 2018. Topics included: Roles and Responsibilities for P/CRCL Officers; Emerging Technologies (License Plate Readers, Facial Recognition, Body Worn Cameras, and Unmanned Aircraft Systems); Auditing Privacy Policies and the role of PCRs; and Operationalizing P/CRCL: Analytic Production. Approximately 75 fusion center personnel representing centers from as far away as Guam, Florida, Vermont, Washington, and many locations in between attended. Privacy Office staff also provided introductory privacy training to 16 new fusion center directors and assistant directors.
- ***International Attaché Training***: The Department's "DHS 201" training module is a week-long course designed to prepare DHS employees who serve as DHS attachés at U.S. embassies worldwide by providing them with basic information on each Component's international activities. The Privacy Office provides an international privacy policy module to raise awareness among new attachés of the potential impact of global privacy policies.
- ***New Employee Orientation***: The Privacy Office provides privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees. Many of the Component Privacy Officers also offer privacy training for new employees in their respective Components. In addition, the Privacy Office provides monthly privacy training as part of the two-day course, *DHS 101*, which is required for all new and existing headquarters staff.
- ***Privacy Briefings for Headquarters Staff***: Upon request or as needed, the Privacy Office provides customized privacy awareness briefings to employees and contractors to

increase awareness of DHS privacy policy and convey the importance of incorporating privacy protections into any new program or system that will collect PII. On November 11, 2018, the Privacy Office Communications Director presented at the Office of the Chief Security Officer (OCSO) Town Hall on best practices to safeguard PII.

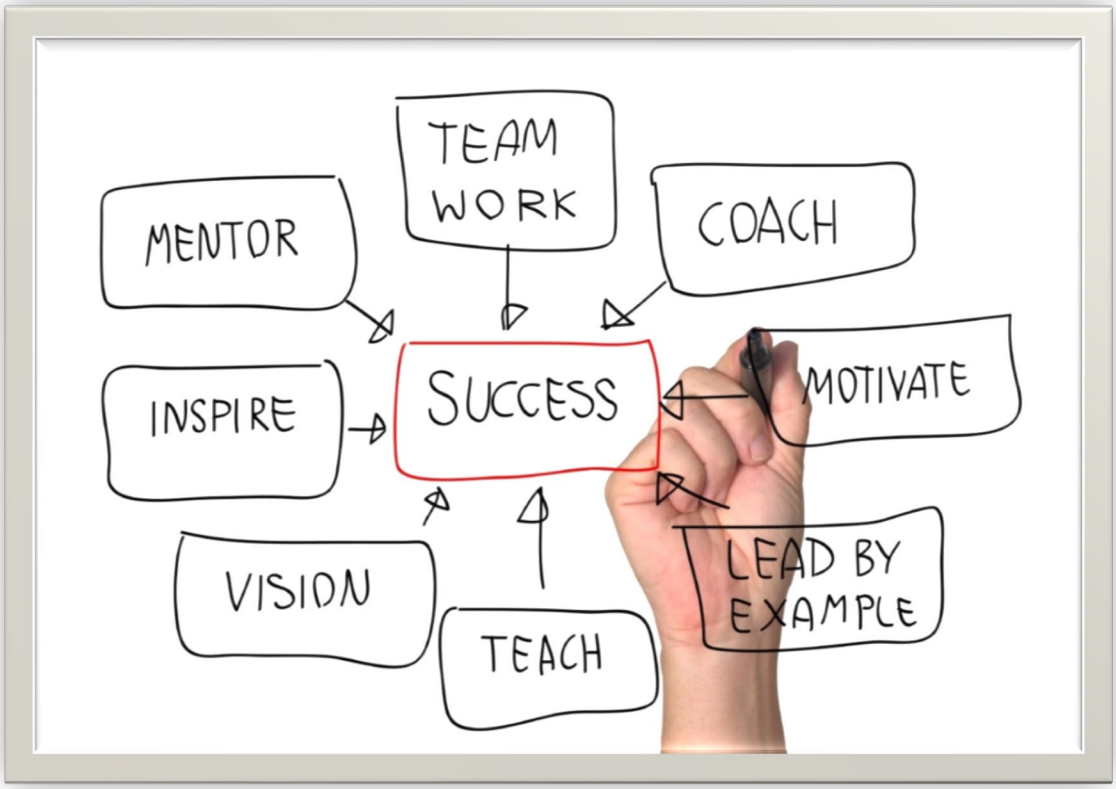
- ***Privacy Office Boot Camp***: The Privacy Office periodically trains new privacy staff in the Components in compliance best practices, including how to draft PTAs, PIAs, and SORNs. The most recent eight-week course was held in Spring 2019.
- ***Reports Officer Certification Courses***: The Privacy Office provides three different privacy training programs to reports officers, senior reports officers, and senior intelligence officers who prepare raw intelligence reports or finished intelligence as part of the DHS Intelligence Enterprise certification program.
- ***Security Specialist Course***: The Privacy Office provides a week-long privacy training program every six weeks to participants from multiple agencies.

Reporting

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

- ***Privacy Office Semi-Annual Section 803 Report to Congress****:* The Privacy Office issues two semi-annual reports to Congress as required by Section 803 of the 9/11 Commission Act,[50] 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 FOIA Officer Report to the Attorney General of the United States***: This report discusses actions taken by the Department to apply the presumption of openness and to ensure that DHS has an effective system to respond to requests, increase proactive disclosures, fully utilize technology, reduce backlogs, and improve response times.
- ***DHS Data Mining Report to Congress***: This report describes DHS activities already deployed or under development that fall within the Federal Agency Data Mining Reporting Act of 2007[51] definition of data mining.
- ***Social Security Number Fraud Prevention Act Report to Congress***: This report documents the Privacy Office's plan to reduce the collection, use, and mailing of SSNs at DHS.
- ***Privacy and Civil Liberties Assessment Reports***: Executive Order 13636 (EO 13636), *Improving Critical Infrastructure Cybersecurity,* and Executive Order 13691 (EO 13691), *Promoting Private Sector Cybersecurity Information Sharing*, require that SAOPs 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.

[50] 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.
[51] 42 U.S.C. § 2000ee-3.



VI. Business Operations

The Privacy Office's FY 2019-2022 Strategic Plan includes:

***Goal Six (Business Operations)*: Efficiently manage business operations, office workflow, human capital, technology, procurement, financial actions, and resilience to ensure the office is fully supported in carrying out its mission.**

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

Workforce

During the reporting period, the Privacy Office hired 11 federal positions, for a total of 40 federal employees, one detailee, one intern, and 17 contractors, including the following back-filled positions:

- Chief of Staff
- Senior Director, Privacy Policy and Oversight
- Attorney Advisor (FOIA)
- Supervisory Government Information Specialist (FOIA)

- Program Analyst (Information Sharing, Safeguarding and Security)
- Two Government Information Specialists (FOIA)
- Senior Government Information Specialist (Policy)
- Two Government Information Specialists (Compliance)
- Correspondence Analyst
- Program and Management Analyst (Student Trainee)

Privacy Office staff also supported the Department's Volunteer Task Force at the Southwest Border. The Privacy Office serves as a strategic partner with the Department's FOIA and Privacy Offices to build a strong pipeline of diverse leaders to enhance DHS privacy and FOIA programs for the future.

Privacy Office staff received numerous commendations for contributing to the Department's FOIA program and were recognized not only by DHS during Sunshine Week, but also by DOJ. In addition, the Director of National Intelligence presented the *Privacy and Civil Liberties Team of the Year Award* to Privacy Office employees for their contributions to the National Vetting Center Privacy, Civil Rights, and Civil Liberties Working Group.

Budget

The Privacy Office's FY 2019 budget of $8,664,000 was allocated as follows:

- 71% personnel compensation and benefits
- 15% working capital fund
- 13% contracts and intra-agency agreements
- 1% travel

The Privacy Office maximized its resources by:

- enhancing operational and financial performance by allowing Components to purchase over $1,000,000 in FOIA and privacy support services using current contract vehicles; this reduced acquisition administrative costs and created time and resource efficiencies;
- leveraging intra-agency agreements with departmental Offices and Components to reimburse the Privacy Office $414,185 for infrastructure and license costs related to FOIAXpress, the web-based application used for processing FOIA and Privacy Act requests;
- creating a separate line of accounting to capture FOIA program costs;
- negotiating with the Office of the Chief Information Officer (OCIO) on cost savings measures for storage and Information System Security Office services;
- expanding telework to reduce carbon footprint and real estate costs; and
- realigning staff to reduce reliance on contract support services.

Staff Training and Development

To build a workforce in which employees can contribute at their highest level, the Privacy Office encouraged its staff, and FOIA and privacy professionals throughout the Department, to seek development opportunities to improve efficiency and productivity. The Privacy Office conducted numerous FOIA and privacy trainings and seminars to emphasize its commitment to developing and maintaining an effective, mission-focused, diverse, and knowledgeable workforce.

Privacy Office staff attended the following training and development opportunities:

- IAPP Global Privacy Summit, April 5-6, 2019, in Washington, DC.
- Biometrics Institute, April 11-12, 2019, in London, United Kingdom.
- Advanced FOIA Training, May 15, 2019, in Washington, DC.
- Society of Human Resources Management, June 23-26, 2019, in Las Vegas, NV.
- American Society of Access Professionals National Annual Training Conference, July 22-24, 2019, in Arlington, VA.

VI. 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 policy[52] 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 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*.

[52] See DHS Privacy Policy Instruction 047-01-005, Component Privacy Officer.

Cybersecurity and Infrastructure Security Agency (CISA)

CISA leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. The CISA Office of Privacy supports several significant activities to promote and protect privacy while supporting critical mission operations at CISA, including the Cybersecurity Division (CSD), Emergency Communications Division (CSD), Infrastructure Security Division (ISD), National Risk Management Center (NRMC), and the Federal Protective Service (FPS). On November 16, 2018, with the enactment of the *Cybersecurity and Infrastructure Security Agency Act of 2018*[53] (CISA Act), OBIM was transferred from CISA to DHS's Management Directorate.

The CISA Act also mandated CISA have a "Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency," working closely with the CPO. Prior to the establishment of CISA, the former National Protection and Programs Directorate (NPPD) had an existing privacy officer and privacy office. The already established NPPD privacy program assumed the privacy responsibilities for CISA.

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

Privacy Leadership

- Conducted two Privacy Oversight Reviews[54] of CISA's cybersecurity programs, specifically focused on CS&C's EINSTEIN intrusion detection system, the Cyber Information Sharing and Collaboration Program (CISCP), and the AIS initiative. During these reviews, the CISA Office of Privacy examined EINSTEIN 2 signatures, CISCP indicator bulletins, and AIS

[53] Pub. Law. No. 115-454.

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

privacy rules to ensure that PII is not collected unnecessarily and is handled appropriately as these programs effectively execute CISA's cybersecurity mission.
- Conducted a self-audit of CISA contributions to the Nationwide SAR Initiative in response to a letter from the DHS CPO. CISA Office of Privacy and the FPS completed a self-audit of its 2018 contributions to eGuardian to ensure its contributions warranted continued retention.
- Conducted DHS's first Component-level Privacy Incident Tabletop Exercise (TTX). Modeled after the Privacy Office's Annual Tabletop Exercise, the CISA TTX trained management-level supervisors in the processes for privacy incident reporting, as well as the steps to mitigate privacy incidents with minimal exposure of personal information and disruption to CISA's mission.
- Participated in the Privacy Office assessments of CISA activities under EO 13636 and 13691.
- Conducted 228 privacy SME 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 CISA Office of Privacy contributed to the federal privacy enterprise through the following activities:
- The CISA Office of Privacy actively engaged with CSD's Federal Network Resilience (FNR) division to update the Federal Incident Reporting Requirements (FIRR), as required by OMB Memo 19-02. The CISA Office of Privacy provided input to the new FIRR (previously known as the Federal Incident Notification Guidelines), connected FNR with appropriate interagency PPOCs, and participated in agency working sessions that assessed agency readiness and capacity to implement the FIRR.
- The CISA Office of Privacy staff are actively engaged with the Federal Privacy Council by attending or participating in its training events and working groups.

Privacy Compliance

As of June 30, 2019, CISA's FISMA privacy score showed that 100 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 100 percent of required SORNs have been completed.

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

Highlights of privacy compliance documents published during the reporting period:

Privacy Impact Assessments:

- DHS/CISA/PIA-023 Infrastructure Protection Gateway: The PIA was updated to describe how the Homeland Security Information Network (HSIN) now acts as an identity proofing service provider to the IP Gateway, and to update language in the IP Gateway System Use Disclaimer.

Federal Emergency Management Agency (FEMA)

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

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

Privacy Leadership

- Initiated and led a FEMA Information Sharing Process and Assessment Initiative to address challenges in determining when, how, and with what tools to securely share PII during disaster operations. The goals of the assessment include identifying gaps in the current information sharing process and establishing a standard process for information sharing with our partners.
- Conducted privacy training for various program offices throughout FEMA to ensure that privacy practices are embedded in agency operations. FEMA Privacy Branch provided both general "Privacy Awareness 101" training as well as role-based training targeted to specific operational needs. Training included:
    - Engaging response and recovery management and leaders at the Office of Response and Recovery (ORR) Leadership Forum;
    - Presenting at the Disaster Workforce Training for the Office of Equal Rights (OER) cadre; and
    - Participating in the Office of External Affairs (OEA) Training Academy.

- 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.
- Represented privacy interests on the Information Governance Working Group (IGWG) as it relates to privacy topics surrounding the use of FEMA SharePoint collaboration sites, to ensure that proper privacy notifications are in place to inform employees how to appropriately protect PII on SharePoint.
- Represented privacy and data protection interests as a permanent voting member of the FEMA Acquisition Review Board, where decisions are made regarding FEMA procurements involving PII. Regularly reviewed acquisition packages for both IT and contracted services procurements to ensure appropriate solicitation/contract clauses and other needed language are included.
- 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.
- Continued to represent privacy and data protection interests as a member of the FEMA Data Governance Council, where decisions are made regarding the use of the agency's data assets involving PII. Collaborated with FEMA Data Governance Council's Data Management Team to conduct privacy training for FEMA data stewards and stakeholders.
- Directly supporting the Administration's Southwest Border Volunteer Force Initiative by providing deployment support using the FEMA Deployment Tracking System (DTS) to assist with deploying and tracking volunteer employee support for this effort.
- Hired and on-boarded three new Senior Privacy Analysts.

Privacy Compliance

As of June 30, 2019, FEMA's FISMA privacy score showed that 100 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 100 percent of required SORNs have been completed.

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

Highlights of privacy compliance documents published during this report period:

Privacy Impact Assessments:

- **DHS/FEMA/PIA-052 Grants Management Modernization (GMM) PIA**: FEMA has developed the GMM Streamlined Platform for Agile Release and Transformation Acceleration (SPARTA) system as part of an IT system modernization effort. Through the development and deployment of the GMM SPARTA system, GMM will streamline grants management across the agency's 40-plus grant programs through a user-centered, business-driven approach. The GMM SPARTA system consolidates the functionalities of FEMA's ten legacy IT systems into a single grants management IT platform.

- **DHS/FEMA/PIA-053 Electronic Document and Records Management System (EDRMS) PIA**: The FEMA Federal Insurance and Mitigation Administration (FIMA) owns and operates EDRMS. FIMA uses EDRMS for document management and records management purposes. FIMA also uses EDRMS for the conversion of paper documents to an electronic format in compliance with the National Archives and Records Administration (NARA) requirements, OMB management of federal records guidance and regulations, and Executive Directives. EDRMS is used as a central storage of FIMA documents that are electronically scanned but are not stored in other FIMA IT systems.

Transportation Security Administration (TSA)

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

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

Privacy Leadership

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

Privacy Compliance

As of June 30, 2019, TSA's FISMA privacy score showed that 100 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 100 percent of required SORNs have been completed.

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

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

U.S. Citizenship and Immigration Services (USCIS)

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

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

Privacy Leadership

- Provided guidance to USCIS's programs and directorates to ensure the implementation of the operational use of social media to protect the privacy, civil rights, and civil liberties of those who will be subject to social media searches;
- Provided privacy risk-based analysis on DHS and government-wide operations, legislative proposals, and EOs;
- Developed and delivered a variety of privacy-related training to USCIS personnel and key stakeholders, including a refresher training on how to identify and protect Section 1367 information within files and electronic systems;
- Developed and implemented a process to ensure that all unauthorized disclosures of Section 1367 information are reported through the privacy incident reporting process and CRCL;
- Developed and launched an agency-wide quiz, Privacy Matters – Test Your Knowledge, in observation of the 2019 Data Privacy Day;
- Assisted the USCIS Avoid Scam working group in their effort to promote identity theft awareness as it relates to telephone scams;

- Developed an external brochure, *Privacy Tips – Internet Safety*, with helpful privacy tips for USCIS customers. The brochure will be published in English and Spanish;
- Developed a Privacy Supervisory Toolkit to assist supervisors locate privacy-related documents and policies. The toolkit will be made available to supervisors on an internal collaboration site;
- Conducted a data protection campaign over the holidays for USCIS personnel located within the northeast region;
- Held a blockchain symposium in Burlington, VT, for USCIS personnel and members of the public;
- Hosted a Spotlight on Privacy for USCIS personnel in District 26 (Honolulu, Hawaii). The event emphasized the legal compliance process as it relates to the development of Locally Developed Applications (LDAs);
- Developed "The Privacy Minute" video series consisting of short, targeted outreach videos disseminated throughout Service Center Operations (SCOPS). The videos address specific privacy messages based on analysis of Significant Incident Reports (SIR) trends and leadership priorities;
- Facilitated information sharing requirements between internal and external stakeholders (federal, state, local, and international organizations) to ensure that such sharing is conducted in compliance with applicable privacy law and policy;
- Integrated privacy by design principles into the IT system development life cycle using a risk-based approach in accordance with NIST guidelines;
- Monitored and reviewed multiple IT development projects to ensure that privacy requirements are considered throughout the Agile lifecycle;
- Conducted 50 site visits to USCIS facilities throughout the country to promote privacy protection best practices related to immigration operations;
- Provided guidance to Contract Officers, Contract Officers' Representatives, and Program Managers on the process for completing the Homeland Security Acquisition Manual Appendix G Form for identifying high-risk contracts; and
- Met with major U.S. courier companies on the appropriate handling of USCIS shipments containing sensitive records to prevent the loss and/or mishandling of USCIS shipments and to ensure compliance with the awarded contract.

Privacy Compliance

As of June 30, 2019, USCIS's FISMA privacy score showed that 96 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 97 percent of required SORNs had been completed.

- Participated in working groups to implement Section 14 of Executive Order 13768, *Enhancing Public Safety in the Interior of the United States*;
- Reviewed over 750 contracts to add privacy clauses, as needed, to protect and secure PII that is shared with USCIS partners; and
- Conducted seven privacy security compliance reviews within USCIS HQ to identify potential privacy and security vulnerabilities and to assess compliance with USCIS and DHS security and privacy policies on securing and safeguarding Sensitive PII and classified information.

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

United States Coast Guard (USCG)

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

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

Privacy Leadership

- Welcomed a new Chief of the Privacy Program;
- Partnered with USCG Office of Commercial Vessel Compliance and launched the TugSafe Inspected Towing Vessels Decision Aid Mobile Application, which provides the commercial maritime industry with a comprehensive tool for determining which regulations are applicable for a specific vessel;
- Collaborated with the USCG Office of C5I Program Management on the Inspect Mobile Application proof of concept. This application provides qualified marine inspectors a secure and effective means of performing a vessel inspection at a remote location, then securely uploads the results into the Marine Information for Safety and Law Enforcement system;
- Provided biweekly training to over 153 new USCG civilian employees, emphasizing the importance of safeguarding PII;
- Collaborated with USCG Forms Manager and Headquarters directorates to conduct a review of all USCG forms containing a SSN data field that are sent via the U.S. Postal Service to external customers and stakeholders. USCG identified 167 forms that met this criterion and determined all were in compliance with the SSN Fraud Prevention Act of 2017;

- Disseminated weekly overviews of current and emergent USCG privacy activities to senior leadership;
- Promulgated an ALCOAST message to the USCG workforce emphasizing the safeguarding of PII on network drives and e-mails;
- Continued monthly meetings with the USCG Health Insurance Portability and Accountability Act (HIPAA) representative to ensure privacy oversight and to mitigate privacy incidents involving personal health information; and
- Created a process to review all ALCOAST messages prior to disseminations, ensuring that all privacy equities, including the need for any privacy compliance documentation, are addressed.

Privacy Compliance

As of June 30, 2019, USCG's FISMA privacy score showed 100 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 100 percent of required SORNs were completed.

- Reviewed USCG directives, forms, and information collection as a part of the clearance process, resulting in the submission of compliance documentation to ensure adherence to current federal privacy mandates and
- Reviewed 110 ITARs, confirming requisite privacy documentation and ensuring core clauses were included in contracted services involving access to PII.

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

Highlights of privacy compliance documents published during the reporting period:

- DHS/USCG/PIA-028 – Defense Sexual Assault Incident Database (DSAID): The Department of Defense (DoD) owns and operates the DSAID system that serves as a centralized, case-level database for military sexual assault reports. The USCG conducted this PIA because the DSAID system collects and maintains PII about USCG personnel and other individuals involved in cases.

- DHS/USCG-008 – Courts-Martial and Military Justice Case Files System of Records: This system of records allows the USCG to collect and maintain records regarding military justice administration and documentation of USCG Courts-Martial proceedings. The USCG renamed this system to "DHS/USCG-008 Courts-Martial and Military Justice Case Files System of Records" and updated this SORN to include new and modified routine uses and remove one existing routine use.

U.S. Customs and Border Protection (CBP)

CBP is one of the world's largest law enforcement organizations, charged with securing our borders while facilitating lawful international travel and trade. As the United States' first unified border entity, CBP takes a comprehensive approach to border management and control, combining customs, immigration, border security, and agricultural protection into one coordinated and supportive activity. The CBP Privacy Office remains heavily engaged in the operational activities of CBP to ensure privacy protections and compliance with all programs.

CBP Privacy conducted the following significant activities during this reporting period:

Privacy Leadership

- Increased outreach and communication with senior leaders within CBP and provided support to numerous high visibility initiatives such as the NVC, biometric exit priorities, and data visualization and AI solutions for big data;
- Reviewed ISAAs for external stakeholder access to CBP IT systems and bulk information sharing requests to ensure that external access to CBP information is consistent with applicable law and the FIPPs;
- Conducted outreach across the CBP enterprise about the importance of safeguarding PII, including providing in-person training to over 2,000 Border Patrol Agents in Laredo, Texas and creating a privacy session as part of the New Employee Orientation training for all new CBP employees;
- Coordinated with SMEs from each of CBP's Operational Components and support offices to review and update CBP's Directive on the Operational Use of Social Media and to draft a Directive on the Maintenance, Use, Sharing, and Protection of Section 1367 'Protected Class' Information; and
- Developed and implemented new SOPs for the office's management of ad-hoc information sharing requests. The SOP provides guidance to the CBP Privacy Office staff in the proper adjudication of information request from federal, state, and local law enforcement agencies.

The SOP helps to ensure that all authorized releases of CBP information in response to these requests are compliant with legal and DHS/CBP policy requirements.

Privacy Compliance

As of June 30, 2019, CBP's FISMA privacy score showed that 100 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 100 percent of required SORNs had been completed.

- Continued to expand the privacy compliance program by requiring PTAs for all forms and information collections, ongoing information sharing initiatives, and all individual sub-systems to improve visibility into what information is being collected, maintained, and shared, and to ensure sufficient PIA and SORN coverage for all IT systems. From July 1, 2018 through June 30, 2019, CBP reviewed over 200 systems, programs, and pilots for privacy risks and compliance requirements;
- Continued to work closely with the CBP Entry and Exit Transformation Office to successfully launch the Traveler Verification Service, providing recommendations for privacy enhancements and publishing several compliance documents in close coordination with the DHS Privacy Office. CBP held several briefings and outreach sessions for advocacy groups on biometric exit initiatives, and supported the DHS Privacy Office and the DPIAC in reviewing CBP's use of biometric facial recognition technology in its entry and exit operations, which culminated in the DPIAC's recommendations report: *Privacy Recommendations in Connection with the Use of Facial Recognition Technology*;
- Collaborated with the CBP Office of Information and Technology to develop a privacy oversight and compliance strategy for systems moving from three-year authorization cycles into ongoing authorization; and
- Fully embedded privacy into all ITARs, as well as all personnel services contract reviews to ensure that all vendors protect CBP information in accordance with federal law and DHS policy.

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

Highlights of privacy compliance documents published during the reporting period:

Privacy Impact Assessments:

- DHS/CBP/PIA-056 Traveler Verification Service (TVS): CBP is congressionally-mandated to deploy a biometric entry/exit system to record arrivals and departures to and from the United States. Following several years of testing and pilots, CBP has successfully operationalized and deployed facial recognition technology, now known as the TVS, to support comprehensive biometric entry and exit procedures in the air, land, and sea environments. CBP issued PIAs documenting each successive phase of TVS testing and deployment; CBP published a comprehensive PIA to consolidate all previously issued PIAs and to provide public notice on how TVS collects and uses PII.

- DHS/CBP/PIA-057 Electronic Secured Adjudication Form Environment (e-SAFE): CBP is tasked with determining the admissibility of all individuals seeking admission into the United States. For non-immigrants seeking admission into the United States, CBP automated the collection of information from visa-exempt citizens of Canada, Palau, Federated States of Micronesia, and the Republic of the Marshall Islands who are eligible to apply for temporary and permanent waivers of inadmissibility through the creation of e-SAFE. CBP published this PIA because waiver applicants may now submit information electronically as part of the waiver application process, and because CBP collects, maintains, and disseminates PII to vet inadmissible non-immigrants applying for a waiver.

- DHS/CBP/PIA-058 Publicly Available Social Media Monitoring and Situational Awareness Initiative: CBP takes steps to ensure the safety of its facilities and personnel from natural disasters, threats of violence, and other harmful events and activities. In support of these efforts, designated CBP personnel monitor publicly available, open source social media to provide situational awareness and to monitor potential threats or dangers to CBP personnel and facility operators. Authorized CBP personnel may collect publicly available information posted on social media sites to create reports and disseminate information related to personnel and facility safety. CBP published this PIA because, as part of this initiative, CBP may incidentally collect, maintain, and disseminate PII over the course of these activities.

U. S. Immigration and Customs Enforcement (ICE)

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

ICE Privacy engaged in the following significant activities during the reporting period:

Privacy Leadership

- Continued to process Privacy Act access and amendment requests received from the FBI Criminal Justice Information Services (CJIS). ICE works with CJIS to ensure that information from ICE, legacy Immigration and Naturalization Service, or legacy U.S. Customs Service arrests maintained in FBI records is accurate and complete;
- Updated our privacy training to ensure that all ICE personnel are effective data stewards; and
- Developed the ICE Implementation Guidance for Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*, as well as training on the policy for ICE personnel involved in making disclosures.

Privacy Compliance

As of June 30, 2019, ICE's FISMA privacy score showed that 100 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 100 percent of required SORNs had been completed.

- Completed or updated 64 PTAs, four PIAs, 14 Disposition PTAs, and 10 Testing Questionnaires during the reporting period;
- Responded to eight Privacy Act amendment requests, and received two privacy complaints;
- Reviewed over 145 proposed procurements to ensure the inclusion of appropriate privacy protections in contract language;
- Resolved an estimated 75 privacy incidents, taking various steps to mitigate any damages from the incidents and prevent future incidents; and

- Provided advice and oversight during the development of seven Information Sharing Agreements signed during the reporting period.

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

Highlights of privacy compliance documents published during the reporting period:

Privacy Impact Assessments:

- DHS-ICE-PIA-049 ICE Parole and Law Enforcement Programs Unit Case Management Systems: The Parole and Law Enforcement Programs Unit (Parole Unit) within ICE Homeland Security Investigations, owns and operates three case management systems: 1) the Parole Case Tracking System (PCTS) to process applications and monitor activities related to law enforcement-requested immigration parolees; 2) the S-Visa System for S-Visa immigration benefits; and 3) the Witness Security (WitSec) System to support the witness security program. These are collectively referred to as the ICE Parole Unit Case Management Systems. The PII maintained in these systems regards 1) aliens otherwise ineligible for admission to the United States who are paroled into the United States in support of law enforcement investigations and activities; 2) aliens either previously removed or currently in removal proceedings who apply for and/or are granted humanitarian parole; and 3) aliens named in applications submitted by law enforcement agencies for participation in the S-Visa and WitSec programs. ICE published this PIA to document and provide transparency on the privacy protections that are in place for the PII contained in the ICE Parole Unit Case Management Systems.

- DHS/ICE/PIA-020 Alien Criminal Response Information Management System (ACRIMe): ACRIMe is an information system used by ICE headquarters and field personnel to receive and respond to immigration status inquiries made by other agencies about individuals arrested, subject to background checks, or otherwise encountered by those agencies. The PIA was updated to document a new ACRIMe Field Module, the renaming of the National Crime Information Center Section Module, new technical services to query other government databases, and to describe the new use of ACRIMe to respond to the U.S. Department of Health and Human Services regarding the immigration status of potential sponsors of unaccompanied alien children.

- DHS/ICE/PIA-015(j) Enforcement Integrated Database (EID) – EAGLE, EDDIE, and DAVID: EID is a DHS shared common database repository used by several DHS law enforcement and homeland security applications. EID stores and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, USCIS, and CBP, all components within DHS. This PIA update addressed the EID Arrest Graphical User Interface (GUI) for Law Enforcement (EAGLE), EAGLE DirecteD Identification Environment (EDDIE), and Digital Application for Victim Witness Identification (DAVID).

- DHS/ICE/PIA-015(i) Enforcement Integrated Database (eHR) System: The EID is a DHS shared common database repository used by several DHS law enforcement and homeland security applications. EID stores and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, USCIS, and CBP. This PIA was updated to reflect changes to information that EID collects and stores, new uses of EID information, and enhanced sharing of EID data.

United States Secret Service (USSS or Secret Service)

The USSS 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.

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

Privacy Leadership

- Continued to take significant steps to implement the PCR recommendations to strengthen USSS Privacy operations and to promote a culture of privacy within the agency, including hiring a dedicated Privacy Officer. This was in response to the 2017 Privacy Office's PCR on USSS privacy practices;
- Created a new program, "Privacy Services Program," and advertised it through posting a new mission, vision, and values intranet statement; a new program logo; updating printed privacy awareness brochures; and creating a new Intranet page dedicated to assisting staff in finding privacy resources, policies, and compliance documents;
- Attended a briefing for U.S. House Subcommittee members on USSS's use of Biometrics;
- Represented privacy and data protection interests as a member of the Enterprise Governance Council, where decisions are made about USSS's funding, procurement, and use of IT assets that involve the collection, use, maintenance, and dissemination of PII;
- Promoted privacy awareness with posters and electronic kiosks throughout the USSS Headquarters building. Sent quarterly service-wide privacy email messages to all USSS staff emphasizing privacy awareness and the proper handling and safeguarding of PII;
- Hosted an inaugural Privacy Town Hall meeting as an annual privacy awareness activity; and
- Established a Breach Response Taskforce to enable the USSS to respond efficiently and effectively to victims of a major privacy incident should one occur.

Privacy Compliance

As of June 30, 2019, USSS's FISMA privacy score showed that 92 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 100 percent of required SORNs had been completed.

- Reviewed and drafted Privacy Act statements for new and existing USSS forms;
- Reviewed IT waiver and/or exception requests submitted by the OCIO for systems processing PII to assess privacy implications;
- Posted privacy banners on SharePoint Forms intranet sites that collect PII to allow the submitter to more readily distinguish forms in which Sensitive PII is or is not allowed;
- Used lessons learned from postal mail incidents to advise business units to change their business processes so that "double-sealed" postal envelopes are now used when the contents include Sensitive PII; and
- Updated a USSS SORN and submitted it through DHS for OMB approval.

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 Infrastructure Security Agency
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 CISA
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
FY	Fiscal Year
GSA	General Services Administration

Acronyms	
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
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
OPM	Office of Personnel Management
P/CL	Privacy and Civil liberties
PCLOB	Privacy and Civil Liberties Oversight Board
PCR	Privacy Compliance Review

Acronyms	
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIHG	DHS Privacy Incident Handling Guidance
PIV	Personal Identity Verification
PLCY	Office of Strategy, Policy, and Plans
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
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;[55]
(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 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.

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

If a PIA is required, the relevant personnel will draft the PIA for review by the Component privacy officer or PPOC and Component counsel. Part of the PIA analysis includes determining whether an existing SORN appropriately covers the activity or a new SORN is required. Once the PIA is approved at the Component level, the Component privacy officer or PPOC submits it to the Privacy Office Compliance Team for review and approval. The CPO signs the final PIA when satisfied with the privacy risk mitigations. Once approved, PIAs are published on the Privacy Office external website, except for 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.[56] 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.[57]

[56] 5 U.S.C. § 552a(e)(4).

[57] 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, 2018 – June 30, 2019		
Component	**Name of System**	**Date Published**
CBP	DHS/CBP/PIA-055 HRM 5000	7/11/2018
CBP	DHS/CBP/PIA-022(a) Border Surveillance Systems (BSS)	8/21/2018
CBP	DHS/CBP/PIA-006(e) Automated Targeting System CIV PIA Addendum	9/21/2018
CBP	DHS/CBP/PIA-056 Traveler Verification Service (TVS)	11/14/2018
CBP	DHS/CBP/PIA-057 Electronic Secured Adjudication Forms Environment (e-SAFE)	3/12/2019
CBP	DHS/CBP/PIA-058 Publicly Available Social Media Monitoring and Situational Awareness	3/25/2019
DHS	DHS/ALL/PIA-067 Continuous Evaluation (CE) Travel Record Data System (TRDS)	8/15/2018
DHS	DHS/ALL/PIA-068 LiveSafe Platform	9/24/2018
DHS	DHS/ALL/PIA-069 DHS Surveys, Interviews, and Focus Groups	9/28/2018
DHS	DHS/ALL/PIA-070 Suspension and Debarment Case Management System	9/28/2018
DHS	DHS/ALL/PIA-071 Office of Immigration Statistics (OIS) Statistical Data Production and Reporting	12/7/2018
DHS	DHS/ALL/PIA-072 National Vetting Center (NVC)	12/11/2018
DHS	DHS/ALL/PIA-060(a) Application Authentication System (AppAuth)	1/30/2019
DHS	DHS/ALL/PIA-073 Electronic Discovery (eDiscovery) Tools for Litigation Use	5/28/2019
ICE	DHS/ICE/PIA-050 Rapid DNA Operational Use	6/25/2019
ICE	DHS/ICE/PIA-051 Law Enforcement Information Sharing Service (LEIS Service)	6/28/2019
ICE	DHS/ICE/PIA-015(j) – EAGLE, EDDIE, AND DAVID	5/14/19
ICE	DHS/ICE/PIA-015(i) Enforcement Integrated Database (EID)	12/3/18
ICE	DHS/ICE/PIA-049 ICE Parole & Law Enforcement Programs Unit Case Management Systems	12/3/18
ICE	DHS/ICE/PIA-020(c) Alien Criminal Response Information Management System (ACRIMe)	9/28/18
CISA	DHS/NPPD/PIA-023(a) Infrastructure Protection Gateway	9/11/2018

Privacy Impact Assessments Published July 1, 2018 – June 30, 2019		
Component	**Name of System**	**Date Published**
S&T	DHS/S&T/PIA-032 Science & Technology Analytical Tracking System (STATS)	7/30/2018
S&T	DHS/S&T/PIA-033 Coastal Surveillance System (CSS)	10/10/2018
S&T	DHS/S&T/PIA-034 Counter Unmanned Aerial Systems (CUAS) Program	11/09/2018
S&T	DHS/S&T/PIA-035 Laboratory Management System (LMS)	12/10/2018
S&T	DHS/S&T/PIA-037 Genomics Informatics System (GIS)	3/8/2019
TSA	DHS/TSA/PIA-049 Office of Inspection Case Management System	7/27/2018
TSA	DHS/TSA/PIA-030(b) Access to Sensitive Security Information (SSI) in Contract Solicitations	2/19/2019
TSA	DHS/TSA/PIA-018(i) Quiet Skies and Silent Partners	4/19/2019
TSA	DHS/TSA/PIA-009 Claims Management System	5/1/2019
TSA	DHS/TSA/PIA-036(a) Canine Website System	5/16/2019
USCG	DHS/USCG/PIA-028 Defense Sexual Assault Incident Database (DSAID)	6/10/2019
USCIS	DHS/USCIS/PIA-023(b) Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)	7/26/2018
USCIS	DHS/USCIS/PIA-073 USCIS and CISOMB Information Sharing	8/02/2018
USCIS	DHS/USCIS/PIA-018(b) Alien Change of Address Card	8/08/2018
USCIS	DHS/USCIS/PIA-060(b) Customer Profile Management System (CPMS)	8/14/2018
USCIS	DHS/USCIS/PIA-057(a) National Appointment Scheduling System	8/27/2018
USCIS	DHS/USCIS/PIA-013-01(a) Fraud Detection and National Security Directorate	9/27/2018
USCIS	DHS/USCIS/PIA-027(d) Asylum Division	9/28/2018
USCIS	DHS/USCIS/PIA-074 IMPACT	10/03/2018
USCIS	DHS/USCIS/PIA-075 RAILS	11/05/2018
USCIS	DHS/USCIS/PIA-056(a) Electronic Immigration System (ELIS)	12/03/2018
USCIS	DHS/USCIS/PIA-009(b) Central Index System (CIS) 2	12/17/2018

Privacy Impact Assessments Published July 1, 2018 – June 30, 2019		
Component	**Name of System**	**Date Published**
USCIS	DHS/USCIS/PIA-076 Continuous Immigration Vetting	2/14/2019
USCIS	DHS/USCIS/PIA-078 Data Streaming Services	3/20/2019
USCIS	DHS/USCIS/PIA-077 FOIA Immigration Records System (FIRST)	3/20/2019
USCIS	DHS/USCIS/PIA-079 Content Management Services (CMS)	5/15/2019
USCIS	DHS/USCIS/PIA-030(g) E-Verify Program	5/17/2019
USCIS	DHS/USCIS/PIA-016(b) Computer Linked Application Information Management System 3 (CLAIMS 3)	5/7/2019
USCIS	DHS/USCIS/PIA-071(a) myUSCIS Account Experience	6/28/2019
USCIS	DHS/USCIS/PIA-080 Enterprise Gateway and Integration Services (EGIS)	6/28/2019
USSS	DHS/USSS/PIA-023 Applicant Lifecycle Information System (ALIS)	8/21/2018
USSS	DHS/USSS/PIA-024 Facial Recognition Pilot	11/26/2018

System of Records Notices Published July 1, 2018 – June 30, 2019		
Component	**Name of System**	**Date Published**
CBP	DHS/CBP-009 Electronic System for Travel Authorization (ESTA)	6/27/2019
CBP	DHS/CBP-022 Electronic Visa Update System (EVUS)	6/27/2019
DHS	DHS/ALL-008 Accounts Receivable Records	12/19/2018
DHS	DHS/ALL-016 Correspondence Records	9/26/2018
DHS	DHS/ALL-018 Administrative Grievance Records	4/29/2019
ICE	DHS/ICE-017 Angel Watch	2/01/2019
TSA	DHS/TSA-001 Transportation Security Enforcement Record System (TSERS)	8/28/2018
USCG	DHS/USCG-008 Court Martial Case Files	5/9/2019
USCIS	DHS/USCIS-011 E-Verify Program	6/18/2019
USCIS	DHS/USCIS-018 Biometric Storage System into the Department of Homeland Security	7/31/2018