Department of Homeland Security

Privacy Office

Fiscal Year 2019 First Semiannual Report to Congress

For the period October 1, 2018 – March 31, 2019

July 10, 2019

Homeland Security

FOREWORD

July 10, 2019

I am pleased to present the U.S. Department of Homeland Security (DHS or Department) Privacy Office's Fiscal Year 2019 First Semiannual Report to Congress, covering the period October 1, 2018 – March 31, 2019.[1]

Highlights

During the reporting period, the Privacy Office:

- Completed 869 privacy reviews, including:
  - 545 Privacy Threshold Analyses;
  - 20 Privacy Impact Assessments; and
  - 3 System of Records Notices.
- Published its *2018 Annual Report to Congress*.

About the Privacy Office

The *Homeland Security Act of 2002* charges the DHS Chief Privacy Officer with primary responsibility for ensuring that privacy protections are integrated into all DHS programs, policies, and procedures. The Chief Privacy Officer serves as the principal advisor to the DHS Secretary on privacy policy.

The *Privacy Act of 1974* (Privacy Act), the *Freedom of Information Act* (FOIA), and the *E-Government Act of 2002* all require DHS to be transparent in its operations and use of information relating to individuals. The Privacy Office centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight, and to support implementation across the Department. The Privacy Office undertakes these statutory and policy-based responsibilities in collaboration with DHS Component privacy[2] and FOIA officers, privacy points of contact (PPOC), and program offices to ensure that all privacy and disclosure issues are afforded the appropriate level of review and expertise.

Please direct any inquiries about this report to the Office of Legislative Affairs at 202-447-5890 or consult our website: www.dhs.gov/privacy.

[1] 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. 42 U.S.C. § 2000ee-1 (2014), Pub. L. No. 113-126, Title III, § 329(b)(4), 128 Stat. 1406 (2014). The DHS Privacy Office semiannual reports cover the following time periods: April – September and October – March.

[2] DHS Components have a Privacy Officer and other DHS offices have a Privacy Point of Contact. A complete list can be found here: http://www.dhs.gov/privacy-office-contacts.

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 following Members of Congress:

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 Jerrold 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

Privacy Office
Fiscal Year 2019
First Semiannual
Section 803 Report to Congress

Table of Contents

LEGISLATIVE LANGUAGE

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007,*[3] as amended, sets forth the following requirements:

"(f) Periodic Reports-

(1) In General –

The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than semiannually, submit a report on the activities of such officers—

(A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;

(ii) to the head of such department, agency, or element; and

(iii) to the Privacy and Civil Liberties Oversight Board; and

(B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) Contents –

Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—

(A) information on the number and types of reviews undertaken;

(B) the type of advice provided and the response given to such advice;

(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and

(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer."

[3] 42 U.S.C. § 2000ee-1(f).

I. PRIVACY REVIEWS

The Privacy Office reviews programs and information technology (IT) systems that may have a privacy impact. For purposes of this report, privacy reviews include the following:

1. Privacy Threshold Analyses, which are the DHS foundational mechanism for reviewing IT systems, programs, and other activities for privacy protection issues to determine whether a more comprehensive analysis is necessary, either through, e.g., by completing a Privacy Impact Assessment or a Systems of Records Notice;
2. Privacy Impact Assessments, as required under the *E-Government Act of 2002,*[4] the *Homeland Security Act of 2002*,[5] and DHS policy;
3. System of Records Notices as required under the *Privacy Act of 1974*, and any associated Final Rules for Privacy Act exemptions;[6]
4. Privacy Act Statements, as required under the Privacy Act,[7] to provide notice to individuals at the point of collection;
5. Computer Matching Agreements, as required under the Privacy Act;[8]
6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*;[9]
7. Privacy Compliance Reviews, per the authority granted to the Chief Privacy Officer by the *Homeland Security Act of 2002*;[10]
8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) Exhibit 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board; and
9. Information Technology Acquisition Reviews;[11] and
10. Other privacy reviews, such as Information Sharing Access Agreement Reviews.

[4] 44 U.S.C. § 3501 note. *See also* OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), *available at*: http://www.whitehouse.gov/omb/memoranda_m03-22.
[5] 6 U.S.C. § 142.
[6] 5 U.S.C. §§ 552a(e)(4), (j), (k). *See also* OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act", 81 Fed. Reg. 94424 (Dec. 23, 2016), available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf.
[7] 5 U.S.C. § 552a(e)(3).
[8] 5 U.S.C. § 552a(o)-(u).
[9] 42 U.S.C. § 2000ee-3.
[10] The Chief Privacy Officer and DHS Privacy Office exercise its authority under Section 222 of the Homeland Security Act (6 U.S.C. § 142) to assure that technologies sustain and do not erode privacy protections through the conduct of PCRs. Consistent with the Privacy Office's unique position as both an advisor and oversight body for the Department's privacy sensitive programs and systems, the PCR is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation.
[11] Section 208 of the E-Government Act requires that agencies conduct a privacy impact assessment (PIA) before procuring information technology (IT) that collects, maintains, or disseminates information that is in an identifiable form. DHS meets this requirement, in part, by participating in the Information Technology Acquisition Review (ITAR) process. The DHS Privacy Office reviews these ITAR requests to determine if the IT acquisitions require a new PIA to identify and mitigate privacy risks or if they are covered by an existing DHS PIA. In addition, the DHS Privacy Office reviews ITAR requests to ensure that appropriate language to safeguard personally identifiable information (PII) and Sensitive PII is included in new and existing contracts and solicitations that have a high risk of unauthorized access to, or disclosure of, sensitive information.

Table I **Privacy Reviews Completed:** ***October 1, 2018 – March 31, 2019***	
Type of Review	***Number of Reviews***
Privacy Threshold Analyses	545
Privacy Impact Assessments	20
System of Records Notices and associated Privacy Act Exemptions	3
Privacy Act (e)(3) Statements[12]	12
Computer Matching Agreements[13]	6
Data Mining Reports	1
Privacy Compliance Reviews	1
Privacy Reviews of IT and Program Budget Requests[14]	40
Information Technology Acquisition Reviews[15] (ITAR)	247
Other Privacy Reviews	0
Total Reviews	***875***

[12] This total does not include all Components; several are permitted to review and approve their own Privacy Act statements by the DHS Privacy Office.
[13] CMAs are typically renewed or re-established.
[14] The Chief Information Officer prepares an annual privacy score as part of its Office of Management and Budget Exhibit 300 reporting. Reviews for this category are reported only during the second semi-annual reporting period.
[15] The DHS Privacy Office initiated ITAR reviews in January 2016.

Privacy Impact Assessments

The Privacy Impact Assessment (PIA) process is one of the Department's key mechanisms to ensure that DHS programs and technologies sustain, and do not erode, privacy protections. In addition to completing PIAs for new systems and projects, programs, pilots, or information sharing arrangements not currently subject to a PIA, the Department also conducts a triennial review of existing PIAs to assess and confirm that the systems still operate within the original parameters. After the triennial review, the Department updates any previously published PIAs, when needed, to inform the public that it has completed a review of the affected systems.

As of March 31, 2019, 100 percent of the Department's Federal Information Security Modernization Act (FISMA) systems that require a PIA had an applicable PIA. During the reporting period, the Office published 20 PIAs: 15 new and 5 updated.

All published DHS PIAs are available on the Privacy Office website, www.dhs.gov/privacy.

Here is a summary of significant PIAs published during the reporting period, along with a hyperlink to the full text.

New Privacy Impact Assessments

DHS/CBP/PIA-056 Traveler Verification Service *(November 15, 2018)*
U.S. Customs and Border Protection (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 Traveler Verification Service (TVS), to support comprehensive biometric entry and exit procedures in the air, land, and sea environments. CBP has issued PIAs documenting each new phase of TVS testing and deployment. CBP issued this comprehensive PIA to a) consolidate all previously issued PIAs; and b) provide notice to the public about how TVS collects and uses personally identifiable information (PII). CBP conducted this overarching, comprehensive PIA for the TVS that has replaced all previous PIAs and provide a consolidated privacy risk assessment for TVS.

DHS/CBP/PIA-058 Publicly Available Social Media Monitoring and Situational Awareness Initiative *(March 25, 2019)*
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 conducted this PIA because, as part of this initiative, CBP may incidentally collect, maintain, and disseminate PII over the course of these activities.

DHS/ICE/PIA-049 ICE Parole and Law Enforcement Programs Unit Case Management Systems *(December 3, 2018)*
The Parole and Law Enforcement Programs Unit (Parole Unit) within U.S. Immigration and Customs Enforcement (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 paroles; 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 is about: 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/S&T/PIA-033 Coastal Surveillance System (CSS) *(October 10, 2018)*
The Science and Technology Directorate (S&T) launched the Coastal Surveillance System (CSS) Pilot program. CSS is a technology demonstration project that establishes a framework (data standards and interfaces) for authorized sharing of data between DHS Components and partners. CSS allows authorized personnel to access information collected by other maritime law enforcement, safety, and security programs. S&T conducted this PIA because CSS collects, maintains, and shares PII from other systems.

DHS/S&T/PIA-034 Counter Unmanned Aircraft Systems Program *(November 9, 2018)*
S&T is leading DHS efforts and coordinating across the Federal Government, testing and evaluating technologies used to detect, identify, and monitor small Unmanned Aircraft Systems (UAS) that may pose a potential threat to covered facilities and assets and other missions authorized to the Department by law. These protective technologies are referred to as Counter-UAS (C-UAS). This PIA discusses measures taken to mitigate privacy risks and protect PII during S&T's testing and evaluation of C-UAS technologies.

DHS/USCIS/PIA-076 Continuous Immigration Vetting *(February 14, 2019)*
In 2017, through an effort known as Continuous Immigration Vetting (CIV), U.S. Citizenship and Immigration Services (USCIS) began vetting 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, to further enhance the agency's ability to identify national security concerns. 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. 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 the time of an initial benefit filing up until naturalization.

DHS/USCIS/PIA-077 FOIA Immigration Records System (FIRST) *(March 20, 2019)*
USCIS operates the *Freedom of Information Act* (FOIA) Immigration Records System (FIRST) to process FOIA requests, Privacy Act requests, and Privacy Act amendment requests from any eligible person or entity requesting access to or amendment of USCIS records. FIRST serves two purposes: (1) FIRST has a public-facing portal that allows members of the public to submit FOIA/Privacy Act requests online, and allows USCIS to electronically deliver responsive records, and (2) FIRST is an internal case management system for USCIS. USCIS conducted this PIA to analyze the privacy impacts associated with USCIS' use of FIRST, as well as the information collected, used, maintained, and disseminated.

DHS/USSS/PIA-024 Facial Recognition Pilot *(November 26, 2018)*
U.S. Secret Service (USSS or Secret Service) is operating a Facial Recognition Pilot (FRP) at the White House complex in order 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 if facial recognition technologies can be of assistance to the USSS in identifying known subjects of interest prior to initial contact with law enforcement at the White House. The 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.

System of Records Notices

The Department publishes System of Records Notices (SORN) consistent with the requirements outlined in the *Privacy Act of 1974*.[16] The Department conducts assessments to ensure that all SORNs remain accurate, up-to-date, and appropriately scoped; that all SORNs are published in the *Federal Register*; and that all significant changes to SORNs are reported to OMB and Congress.

As of March 31, 2019, 100 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the Office published two SORNs: one new and one updated, and one Privacy Act rulemaking.

All DHS SORNs and Privacy Act rulemakings are available on the Privacy Office website, www.dhs.gov/privacy.

Here is a summary of significant SORNs published during the reporting period, along with a hyperlink to the full text in the *Federal Register*.

New System of Records Notices

DHS/ICE-017 Angel Watch Program
Angel Watch Program is used to collect information on covered sex offenders to: (1) combat transnational child sex tourism or exploitation; (2) share information on covered sex offenders with foreign countries to aid them in making informed decisions regarding the admissibility of travelers in their own countries; (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. *(84 Fed. Reg. 1182, March 4, 2019)*

Updated System of Records Notices

DHS/ALL-008 Accounts Receivable System of Records
This system of records describes DHS's collection and maintenance of records on accounts receivable, which enables DHS to have an accurate accounting of money it is owed. DHS updated the SORN to clarify the authorities for collection; and expand the record source categories, categories of individuals, and categories of records. DHS also modified routine use E and added routine use F to comply with the Office of Management and Budget (OMB) Memorandum M-17-12. This notice also updated the system location, and included non-substantive changes to simplify the formatting and text of the previously published notice. *(83 Fed. Reg. 65176, December 19, 2018)*

[16] 5 U.S.C. §§ 552a(e)(4), (j), (k). *See also* OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," 81 Fed. Reg. 94424 (Dec. 23, 2016), available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf.

Privacy Compliance Reviews

The DHS Privacy Office serves as both an advisor and oversight body for the Department's privacy-sensitive programs and systems. The Privacy Compliance Review (PCR) was designed as a collaborative effort to help improve a program's ability to comply with existing privacy compliance documentation, including PIAs, SORNs, and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreements. A PCR may result in a public report or internal recommendations, depending upon the sensitivity of the program under review.

DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews implements DHS Directive 047-01, "Privacy Policy and Compliance," with regard to the Component Head's responsibility to assist the Chief Privacy Officer (CPO) in reviewing Component activities to ensure that privacy protections are fully integrated into Component operations.

The Privacy Office published one PCR during this reporting period. All public PCRs are available on the Privacy Office website, www.dhs.gov/privacy, under Privacy Oversight.

Section 1367 Privacy Incidents

In November 2018, the DHS Privacy Office conducted a PCR to assist certain Components in identifying and mitigating 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 Components' privacy protections and made four recommendations of best practices to prevent and mitigate future privacy incidents affecting individuals protected by Section 1367.

II. ADVICE AND RESPONSES

The Privacy Office provides privacy policy leadership on a wide range of topics in various fora, as described in detail in the *2018 Privacy Office Annual Report* cited below.

Highlights of significant accomplishments during this reporting period are summarized below.

Privacy Policy Initiatives

New Privacy Council

To facilitate the policy review process and foster implementation among the Components, the Chief Privacy Officer stood up a Privacy Council in October 2018. The general membership is comprised of Component Privacy Officers who meet monthly to review and discuss new or revised privacy policies and other key issues.

New Social Security Number Reduction Policy

The Privacy Office will soon implement a new Department policy requiring the elimination of the unnecessary collection, use, maintenance and dissemination of the Social Security number (SSN) by DHS programs, systems, and forms. Where feasible, the SSN will be replaced by a unique alternative identifier.

Privacy Incident Tabletop Exercise

In April, the Privacy Office hosted, in conjunction with the Federal Emergency Management Agency's (FEMA) National Exercise Division, the second Annual DHS Privacy Incident Tabletop Exercise in Washington, DC. This facilitated exercise examined: 1) key DHS decisions required to address minor and major privacy incidents; and 2) the roles and responsibilities of all members of the Breach Response Team as outlined in the DHS Privacy Incident Handling Guidance.

Publications

The Privacy Office published the following congressional reports during this reporting period:

- 2018 Privacy Office Annual Report
- Second annual report to Congress concerning the use of Social Security Numbers (SSNs) in mailed correspondence, as required by section 2(c)(4) of the *Social Security Number Fraud Prevention Act of 2017*
- 2018 Executive Order 13636 and 13691 Privacy and Civil Liberties Assessment Report
- 2017 Data Mining Report

III. Training and Outreach

Mandatory Online Training

105,103 DHS personnel completed the mandatory computer-assisted 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.

988 DHS personnel completed Operational Use of Social Media Training during this reporting period, as required by *DHS Directive Instruction Number 110-01-001, Privacy Policy for Operational Use of Social Media*, and applicable Privacy Office-adjudicated Component Social Media Operational Use Template(s).

Classroom Training

2,896 DHS personnel attended instructor-led privacy training courses, including the following for which the Privacy Office either sponsored or provided a trainer:

- ***FOIA Training***: This periodic training is tailored to FOIA staff throughout the agency responsible for processing FOIA requests.
- ***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 Privacy and Civil Right and Civil Liberties 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. Earlier, Privacy Office staff 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 the importance of protecting 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.

- ***Reports Officer Certification Course*:** The Privacy Office provides privacy training to reports officers who prepare intelligence reports as part of the DHS Intelligence Enterprise certification program.
- ***Security Specialist Course*:** The Privacy Office provides privacy training every six weeks to participants of this week-long training program, who represent multiple agencies.

DHS Privacy Office Outreach

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

- **Certified InfoSec Conference**: On October 10, 2018, the Acting Chief Privacy Officer delivered the keynote address for the data privacy track entitled: *Where Are We in the American Privacy Movement?*
- **National Defense Industrial Association Meeting**: On October 17, 2018, the former Chief Privacy Officer presented on *Privacy Programs and the General Data Protection Regulation.*
- **Data Privacy and Integrity Advisory Committee (DPIAC) Meeting**: On December 10, 2018, a public meeting was held 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*.
- **Cybersecurity: Protecting Sensitive Information**: On February 19, 2019, the Acting Chief Privacy Officer was a panelist at this workshop hosted by Sheppard Mullin.
- **RSA Conference**: On March 5, 2019, the Acting Chief Privacy Officer moderated a panel discussion: *Use of Facial Recognition to Combat Terrorism and Make International Travel More Secure.*
- **Federal Privacy Council's Privacy Boot Camp**: On March 11, 2019, the Acting Chief Privacy Officer gave a presentation: *Privacy 101: Privacy at a Federal Agency.*

DHS Component Privacy Office Training and Outreach

This section features proactive steps taken by DHS Component Privacy Offices to educate and inform DHS staff on privacy law and policy.

Cybersecurity and Infrastructure Security Agency (CISA)

- Provided a Privacy Briefing during New Employee Orientation to all new employees during the reporting period.
- Provided privacy briefings on the Paperwork Reduction Act and Information Technology Acquisition Reviews as part of the CISA IT Security Summit.
- Provided role-based privacy training to CISA Regional Chiefs of Protective Security and Regional Readiness Branch Protective Security Advisors.
- Published two privacy-related articles in CISA's weekly newsletter, *CISA Vision,* and two issues of the quarterly privacy newsletter, *CISA Privacy Update.* The newsletter is distributed CISA-wide and posted on the CISA Office of Privacy internal intranet page.

Federal Emergency Management Agency (FEMA)

- Conducted in-person Privacy 101 (general privacy awareness) training to several FEMA components and offices, to include Mission Support, Region 1, and Office of the Chief Human Capital Officer. These trainings were provided upon request from the office or as part of proactive outreach efforts.
- Trained the Office of Equal Rights disaster cadre during their Mission Rehearsal Training at the Center for Disaster Preparedness. Topics included the handling of sensitive Equal Employment Opportunity and civil rights data, and information sharing within FEMA.

Science & Technology Directorate (S&T)

- Revamped S&T's Privacy 101 training presentation to use in proactive outreach efforts across the directorate.
- Conducted in-person Privacy 101 training sessions to S&T's Office of Innovation and Collaboration; Border, Immigration, and Maritime division; First Responders and Detection division and the Communications Outreach division.
- Developed privacy guidelines to be reviewed when submitting new contracts through the PR tracker. Privacy guidelines identified PII/SPII and privacy sensitive technologies that would require privacy review.
- Published privacy-related article in S&T's weekly newsletter.

Transportation Security Administration (TSA)

TSA Privacy conducted outreach activities with over 350 personnel and members of the public during the reporting period, including:

- Hosted a Multicultural Roundtable with TSA stakeholders and advocates from Sikh American Legal Defense and Education Fund, National Center for Transgender Equality, Hindu American Foundation, and others.
- Collaborated with the Human Capital Town Hall to provide technical training on SharePoint access controls and permissions settings.
- Presented at TSA's Biometrics Industry Day on privacy compliance to private sector stakeholders and privacy advocates.

U.S. Customs and Border Protection (CBP)

- Issued a number of notices to the workforce on information protection and sharing processes and procedures.
- Conducted site visits with Ports of Entry and Border Patrol Sectors to discuss privacy issues and concerns.
- Participated on a panel discussion of the government's use of facial recognition technology to facilitate a large-scale transformation of international travel to and from the United States during the 2019 RSA Cyber Security conference in San Francisco, CA.

U. S. Citizenship and Immigration Services (USCIS)

- 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 for USCIS personnel located within the Northeast area.
- Held a block chain 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 put emphasis on the legal compliance process as it relates to the development of Locally Developed Applications (LDAs).
- Developed *The Privacy Minute*, short, targeted outreach videos disseminated throughout Service Center Operations (SCOPS). The videos address specific privacy messages based on an analysis of Significant Incident Reports (SIRs) trends and leadership priorities.

U. S. Coast Guard (USCG)

- Trained all new employees on the importance of protecting personal information.
- Distributed an ALCOAST message as a reminder to the Coast Guard workforce that PII and sensitive PII must be protected using the appropriate safeguards.

U. S. Secret Service (USSS)

- Trained all new employees and contractors prior to accessing USSS technology and equipment on DHS and USSS privacy resources and requirements related to the proper handling and safeguarding of PII/SPII.
- Sent a service-wide privacy message each quarter to all USSS employees emphasizing privacy awareness and the proper handling and safeguarding of PII/SPII. The first quarter message emphasized the importance of data minimization; the second quarter message emphasized proper PII submission in SharePoint forms.
- Attended a privacy incident table-top exercise hosted by the USSS Deputy Chief Information Security Officer. The exercise entailed a breach of PII during a security event, thus offering those in attendance lessons learned, and established executive roles in the event of an actual incident.
- Posted a new USSS intranet article regarding the program's new mission, vision, and values; introduced a new program logo; updated printed brochures; and created a new Intranet page to assist staff in finding privacy resources and support.
- Presented to USSS staff from various offices on proper PII safeguards and tools to use when returning data to the Annual Financial Management Audit.
- Mitigated spills and breaches from SharePoint Forms by increasing the banners on SharePoint portals that collect PII to more readily distinguish for the submitter forms in which Sensitive PII was/was not allowed.

IV. Privacy Complaints and Dispositions

For purposes of Section 803 reporting, complaints are written allegations of harm or violations of privacy compliance requirements that are filed with the DHS Privacy Office or DHS Components by U.S. citizens, Lawful Permanent Residents, visitors, and aliens.[17]

Privacy Complaints Received by DHS Components and the DHS Traveler Redress Inquiry Program *October 1, 2018 – March 31, 2019*										
Type	**CBP**	**CISA**	**FEMA**	**ICE**	**TSA**	**USCG**	**USCIS**	**USSS**	**TRIP**	**TOTALS**
Procedure	422	0	0	0	9	0	0	0		431
Redress	59	0	0	0	0	0	0	0	5	64
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**	**5**	**3,153**

DHS separates 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 System of Records Notices.
    a. *Example*: An individual alleges that a program violates privacy by collecting Social Security numbers 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 Traveler Redress Inquiry Program (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 Social Security number.

In addition, the Privacy Office reviews redress complaints received by 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.

[17] *See* DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*, available here https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

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 – March 31, 2019, **470** travelers checked the privacy box. Of the 470 complaints, only one of them fit the exact criteria above. An additional five complaints had a general privacy nexus (one – DHS loss of control; four - DHS data integrity).