Department of Homeland Security

Privacy Office

Fiscal Year 2019 Second Semiannual Report to Congress

For the period April 1 – September 30, 2019

January 22, 2020

Homeland Security

FOREWORD

January 22, 2020

I am pleased to present the U.S. Department of Homeland Security (DHS or Department) Privacy Office's Fiscal Year 2019 Second Semiannual Report to Congress, covering the period April 1 – September 30, 2019.[1]

Highlights

During the reporting period, the Privacy Office:

- Completed **1,255** privacy reviews, including:
  - 700 Privacy Threshold Analyses;
  - 33 Privacy Impact Assessments; and
  - 8 System of Records Notices.
- Published its *2019 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 Michael Pence
President, U.S. Senate

The Honorable Nancy Pelosi
Speaker, U.S. House of Representatives

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 Carolyn Maloney
Chairman, Acting, 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
Second 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, e.g., either through 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:** ***April 1 – September 30, 2019***	
Type of Review	***Number of Reviews***
Privacy Threshold Analyses	700
Privacy Impact Assessments	33
System of Records Notices and associated Privacy Act Exemptions	8
Privacy Act (e)(3) Statements[12]	4
Computer Matching Agreements[13]	6
Data Mining Reports	0
Privacy Compliance Reviews	2
Privacy Reviews of IT and Program Budget Requests[14]	45
Information Technology Acquisition Reviews[15] (ITAR)	457
Other Privacy Reviews	0
Total Reviews	***1,255***

[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 September 30, 2019, 99 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 33 PIAs: 17 new and 16 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/ICE/PIA-050 Rapid DNA Operational Use (*June 25, 2019*)
U.S. Immigration and Customs Enforcement (ICE) uses 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. ICE conducted this PIA 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;
- outline the privacy risks involved in using Rapid DNA technology; and
- explain how ICE will mitigate privacy risks.

DHS/CISA/PIA-031 Small Unmanned Aircraft Systems (sUAS) *(July 25, 2019)*
The Cybersecurity and Infrastructure Security Agency (CISA) Infrastructure Security (IS) Division incorporates the use of sUAS into its program offering exercises to critical infrastructure protection stakeholders to train for, assess, practice, and improve performance in prevention, protection, mitigation, response, and recovery capabilities for natural or man-made attacks. Uses during exercises include capturing photographic and video images of the exercise activities, and to use the sUAS as a simulated payload delivery mechanism for certain exercise scenarios. CISA conducted this PIA to address the privacy impacts of the sUAS image capturing capabilities.

DHS/ALL/PIA-074 Chief Human Capital Officer DHS Volunteer Force (*July 8, 2019*)
DHS is recruiting federal employees from all DHS Components and from other federal agencies for the DHS Volunteer Force (DVF), a program that deploys volunteers to the southern border and other locations to help respond to a humanitarian and security crisis. DVF volunteers support U.S. Customs and Border Protection (CBP) or ICE in those DHS Components' efforts to respond to the border crisis, and to stabilize the region. CBP volunteers are assigned to one of five roles that provide services to migrants and detainees: meal distribution, medical assessment, hospital watch, personal property management, or high capacity transport. ICE volunteers are either federal attorneys that help manage

ICE's immigration litigation case load, or federal health care professionals that help evaluate and treat ICE detainees. DHS conducted this PIA because the systems and processes that support the DVF program collect, use, store, and share PII and Sensitive PII.

DHS/ALL/PIA-075 Office of the Chief Human Capital Officer Workforce Analytics and Employee Records (*September 27, 2019*)
Workforce Analytics and Employee Records is a federal human capital business function, whereby federal agencies implement a systematic process to review workforce performance data, metrics, and results. Federal agencies conduct these reviews in an effort to anticipate and plan for future strategic and operational requirements, and to make holistically informed human capital management decisions. Specifically, federal human capital organizations generate evidence-based metrics to support decision-making concerning recruitment, staffing, training, and workforce development. The Workforce Analytics and Employee Records Business Function also facilitates compensation and benefits modeling, as well as the application of statistical models on such human resources issues as retention rates, time to on-board, retirement trends, and employee engagement. DHS conducted this PIA because the systems and data sources that support Workforce Analytics and Employee Records at DHS collect, use, store, and transmit PII and Sensitive PII.

Updated Privacy Impact Assessments

DHS/TSA/PIA-018(i) Silent Partner and Quiet Skies (*April 19, 2019*)
The Transportation Security Administration (TSA) leverages its access to CBP's Automated Targeting System (ATS) to identify individuals for enhanced screening during air travel through the 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 the 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 that TSA can take appropriate actions to address and mitigate that risk. This PIA was updated to reflect operational and administrative changes to the TSA Secure Flight Program.

DHS/USCIS/PIA-013-01(a) Fraud Detection and National Security Directorate (*July 26, 2019*)
The U.S. Citizenship and Immigration Services (USCIS) updated the PIA for the Fraud Detection and National Security Directorate (FDNS), published on December 16, 2014, to discuss changes to the process for accessing social media information when conducting certain background, identity, and security checks. Primarily, this relates to the use of fictitious accounts or identities in certain instances, when access to publicly-available information is only available to those who have a social media account. USCIS will only access social media content that is publicly available to all users of the social media platform.

DHS/TSA/PIA-046(a) Travel Document Checker Automation Using Facial Recognition (*August 23, 2019*)
TSA conducted a short-term proof of concept at the McCarran International Airport (LAS) for automating the identity verification portion of the Travel Document Checker (TDC) using biometric technology. TSA assessed its ability to compare the passenger's live facial image at the checkpoint against an image taken from the passenger's identity document for passengers who opted to participate. This information will be used for subsequent qualitative and quantitative analysis by the DHS Science and Technology (S&T) Directorate. This PIA follows TSA's previously published PIA, which covered a proof of concept at the Los Angeles International Airport (LAX) for automating the identity verification portion of the TDC using facial recognition technology to capture a passenger's facial image to compare against the biometric image contained on the passenger's e-Passport. This PIA was conducted pursuant to Section 222 of the *Homeland Security Act* to address the privacy risks inherent in the use of facial recognition technology during this pilot.

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 September 30, 2019, 100 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the Office published six updated SORNs and two Privacy Act rulemaking(s).

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*.

Updated System of Records Notices

DHS/ALL-018 Administrative Grievance Records

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. The records are used by the Department to resolve employee concerns about working conditions, the administration of collective bargaining agreements, employee/supervisor relations, work processes, and other similar issues. *(84 Fed. Reg. 18070, April 29, 2019)*

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

This system of records outlines how the United States Coast Guard (USCG) collects and maintains records regarding military justice administration and documentation of USCG court martial proceedings. *(84 Fed. Reg. 20383, May 9, 2019)*

DHS/USCIS-011 E-Verify Program

The purpose of this system is to provide employment authorization information to employers, entities authorized by federal law to participate in E-Verify, and to individuals seeking to check employment eligibility under the Immigration and Nationality Act (INA). This system also enables individuals to access features concerning the use of their PII in E-Verify, such as the ability to lock their Social Security number (SSN) to prevent its use in E-Verify and Self Check. The system may also be used by DHS to support DHS monitoring and compliance activities for obtaining information in order to prevent the commission of fraud, discrimination, or other misuse or abuse of the E-Verify system, including violations of privacy laws or other illegal activity, for example: (1) duplicate or incomplete enrollments by employers; (2) inappropriate enrollments by individuals posing as employers; (3) verifications that are not performed within the required time limits; and (4) cases referred by and between E-Verify and the Department of Justice Immigrant and Employee Rights Section (formerly known as the Office of Special Counsel for Immigration-Related Unfair Employment Practices), or other intelligence or law enforcement entities. *(84 Fed. Reg. 28326, June 18, 2019)*

[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.

DHS/CBP-022 Electronic Visa Update System (EVUS)
The purpose of this system is to permit CBP to collect and maintain records on travelers who hold a passport issued by an country identified for inclusion in the EVUS program as selected by the Secretary of Homeland Security, and who have been issued a U.S. nonimmigrant visa of a designated category, in order to determine whether any of those enrollees pose a security risk to the United States over the duration of the visa. *(84 Fed. Reg. 30751, June 27, 2019)*

DHS/CBP-009 Electronic System for Travel Authorization (ESTA)
This SORN describes CBP's collection and maintenance of records that pertain to eligible international travelers who wish to travel to the United States under the Visa Waiver Program and have applied for an ESTA travel authorization, and persons whose information is provided in response to an ESTA application or Form I-94W questions. *(84 Fed. Reg. 30746, June 27, 2019)*

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. *DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews* implements DHS Directive 047-01, "Privacy Policy and Compliance," regarding 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.

A PCR may result in a public report or internal recommendations, depending upon the sensitivity of the program under review. The Privacy Office published two PCRs during this reporting period. All public PCRs are available on the Privacy Office website, www.dhs.gov/privacy, under Privacy Oversight.

Countering Violent Extremism Grant Program

Beginning in 2016, the former Office of Community Partnerships and the Federal Emergency Management Agency (FEMA) managed the Countering Violent Extremism Grant Program (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 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 from its initial 2016 funding, the findings reflected in this report serve as lessons learned that the Office for Targeted Violence and Terrorism Prevention (TVTP) should carefully consider for any future CVEGP iterations, if applicable. Further, the FEMA Grant Programs Directorate, as the administrator and manager of DHS grants, should fully implement the Privacy Office's recommendations to improve privacy protections for any future grant program that includes a security review. *May 2019*

Key findings include:

1. *Sufficient and timely notice regarding the potential to undergo a security review as part of the CVE grant review process, and what that would entail, was not provided.*
2. *Grant applicants were not provided detailed notice nor timely consent opportunities when undergoing a security review as part of the CVEGP application process.*

DHS Science and Technology Directorate

This PCR was conducted under the Chief Privacy Officer's authority in accordance with Section 222 of the *Homeland Security Act of 2002*, because of growing concerns that S&T's privacy compliance process, particularly for those programs involving social media and volunteers, did not meet requirements under DHS policies. The PCR found that S&T requires significant resources to have an effective privacy program that incorporates robust compliance, oversight, outreach, and collaboration, and made six recommendations to improve its privacy posture. *June 2019'*

1. Of six findings, the key finding was: *S&T should promptly reorganize the S&T Privacy Office and fully comply with DHS Instruction 047-01-005.*

II. ADVICE AND RESPONSES

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

Privacy Officer Recommendations

The Privacy Office initiated a new process whereby additional recommendations to mitigate privacy risk are included in certain Privacy Impact Assessments. The first PIA to include "DHS Privacy Office Recommendations" is DHS/USCIS/PIA-013-01(a), *Fraud Detection and National Security Directorate (Social Media)*, and it contains seven recommendations.

Privacy Policy Initiatives

New Social Security Number Reduction Policy

The Privacy Office 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.

Privacy Incident 2019 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 and Privacy Policy Instruction 047-01-006 Privacy Incident Responsibilities and Breach Response Team.

Privacy Policy Assessment Project

The 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 new and existing policies, directives, and instructions.

Publications

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

- *2019 Privacy Office Annual Report to Congress*
- *2019 Social Security Number Fraud Prevention Act Report to Congress*

III. Training and Outreach

Mandatory Online Training

160,239 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.

4,080 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

5,880 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. During this reporting period the following special FOIA training or event was sponsored by the Privacy Office or a DHS Component:
  - May 15, 2019 - Advanced FOIA Training: Training targeted to DHS FOIA professionals with at least one year of experience.
  - June 4, 2019 - Dispute Resolution Skills with the Office of Government Information Services: Training targeted to DHS FOIA professionals, including FOIA Public Liaisons, who regularly interact with requesters.
  - June 18, 2018 - Litigation Training with Dick Huff: Training targeted to DHS FOIA professionals with litigation responsibilities, or processors looking for insight into litigation concerns.
  - June 26, 2019 - Requester Brownbag with the co-founder of MuckRock: Training targeted to DHS FOIA professionals who are interested in learning more about MuckRock and requester perspectives.
- ***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.
- ***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.

- **International Association of Privacy Professionals (IAPP) Global Summit**: May 3-4, 2019, in Washington, DC, the Acting 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*.
- **American Society for Access Professionals 2019 Privacy Program**: In June 2019, in Washington D.C., the Senior Director for Privacy Policy and Oversight took part in a panel discussion about the challenges inherent in keeping privacy programs relevant and compliant in today's ever-changing technical environment.
- **American Society for Access Professionals National Training Conference**: July 22-24, 2019, in Arlington, VA. The Acting CPO participated on a panel with representatives from the Departments of State and Transportation, leading a discussion on several privacy incident scenarios relevant to FOIA professionals.
- **Luncheon sponsored by the Association for Federal Enterprise Risk Management (AFERM) and the Information Systems Audit and Control Association (ISACA)**: On August 14, 2019, in Washington, DC, the Acting CPO participated on a panel discussion with the CPO from the Internal Revenue Service on *Privacy Risk and Enterprise Risk Management.*
- **Federal Privacy Council's Privacy Bootcamp:** In September 2019, in Washington, DC, the Senior Directors for both Privacy Compliance and Privacy Policy & Oversight presented on mobile applications and privacy and the privacy compliance artifacts at this semi-annual course for new privacy professionals in the Federal Government.

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.
- Provided role-based privacy training to the Federal Protection Service Personnel Security Division.
- Trained Executive Secretariat employees on how to safeguard PII when handling correspondence.
- 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 FIMA, Office of External Affairs, Office of the Chief Human Capital Officer, and the Tallahassee, Florida Joint Field Office. These trainings were provided upon request from the office or as part of proactive outreach efforts.
- Trained the Office of Policy and Program Analysis (OPPA) to broaden awareness of privacy laws and policies related to the development of a new system of record, FEMADex.
- Led an Information (PII/SPII) Sharing Process and Assessment effort tasked with reviewing FEMA's information sharing practices, creating a standardized process, and assessing PII/SPII sharing agreements through FEMA.

Science & Technology Directorate (S&T)

- DHS personnel completed instructor- led privacy training and awareness briefings with the following S&T Offices and Programs:
    - Data Analytics Technology Center
    - Biometrics and Identity Technology Center
    - Office of National Laboratories Leadership, to include:
        - National Bio and Agro-Defense Facility
        - National Urban Security Technology Laboratory
        - Plum Island Animal Disease Center
        - Transportation Security Laboratory
        - Chemical Security Analysis Center
    - DHS federally-funded research and development centers:
        - National Biodefense Analysis and Counter Measures Center
        - Homeland Security Systems and Engineering Development Institute
    - University Programs Center of Excellence for Texas A&M
    - Office of International Partnerships
    - Office of Industry Partnerships/Silicon Valley Innovation Program
    - HSAR 15-01/Appendix G Privacy Review Training for expanding awareness to S&T Privacy Office personnel
    - Delivered classroom Privacy 101 Training to S&T executive and principal directors
    - Delivered the S&T Privacy Strategic Review, including privacy training, to the entire S&T leadership staff. The class included information on the S&T Privacy Office roles and

responsibilities, and how to integrate privacy compliance into S&T programs, projects, and activities.

- Drafted and distributed a new privacy awareness brochure throughout S&T.
- Participated in S&T Paperwork Reduction Act Compliance in person training to discuss S&T privacy compliance convergence with Paperwork Reduction Act (PRA) Compliance.

Transportation Security Administration (TSA)

- Conducted a webinar on how to set appropriate user access permissions on internal iShare websites to 165 human capital employees to assist in preventing unauthorized access to data.
- Conducted privacy training as part of the PRA process to 50 employees.

U. S. Citizenship and Immigration Services (USCIS)

- Promoted privacy awareness among employees via email, posters, and digital messages on TV monitors in all facilities.

U. S. Coast Guard (USCG)

- Continued its privacy presentations at the biweekly USCG Civilian Employee Orientation session. USCG Privacy focused on raising awareness of the importance of protecting personal information while assigned to DHS. In addition, USCG Privacy provided and discussed policy outlined in the DHS factsheet titled *How to Safeguard Sensitive PII*.
- Participated in the Second Annual DHS Privacy Incident Tabletop Exercise in Washington, DC, on April 10, 2019. During this exercise, USCG Privacy provided information regarding gaps and issues in the privacy incident handling process.
- Created and disseminated a flyer emphasizing the requirements and instructions for encrypting or password-protecting electronically-sensitive information. This flyer is also provided to commands who are remediating incidents involving unauthorized release of un-encrypted or non-password protected PII and Sensitive PII.
- Attended the USCG Contracting Officer Representatives (COR) Conference in Baltimore, MD, on July 25, 2019, and briefed contractor responsibilities for properly safeguarding PII, emphasizing the integration of privacy compliance in all aspects of the contracting process.
- Initiated an awareness campaign consisting of periodic "privacy tips" on the Coast Guard Portal Special Notices page and information screens located at building entrances, cafeterias, and lunch rooms.

U.S. Immigration and Customs Enforcement (ICE)

- The Acting ICE Privacy Officer presented ICE's Implementation Guidance on DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding the Collection, Use, Retention, and Dissemination of Personally Identifiable Information,* at the Second Annual DHS Information Law Symposium on June 18, 2019, for approximately 85 DHS employees.

U. S. Secret Service (USSS)

- Presented at the annual Special Agent in Charge Conference on data privacy and information stewardship and the role of the Privacy Services Program.
- Promoted privacy awareness with posters and electronic kiosks throughout the USSS Headquarters building. Sent two quarterly service-wide email messages to all USSS staff emphasizing mandatory training responsibilities for privacy courses, and another for safeguarding privacy and incident reporting.
- Prepared presentation materials for and hosted an inaugural "Privacy Town Hall" meeting as an annual privacy awareness activity.
- Constituted, prepared materials for, and led the first-ever USSS Breach Response Team such that USSS can respond efficiently and effectively to victims of a major privacy breach.
- Trained the Human Resources Office on how to safeguard PII.
- Trained contractors on the rules of behavior for the operational use of social media.

IV. 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*, 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.

U.S. citizens, Lawful Permanent Residents, visitors to the United States, and aliens may submit privacy complaints to the Department.[17] The Privacy Office also reviews and responds to privacy complaints referred by employees throughout the Department, or submitted by other government agencies, the private sector, or the public. DHS Components manage and customize their privacy complaint handling processes to align with their specific missions, and to comply with Department complaint handling and reporting requirements.

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 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 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.

[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 April 1 – September 30, 2019, 296 travelers checked the privacy box but none of them were determined to fit the exact criteria above. However, 19 were determined to have a general privacy nexus; one was sent to TSA Privacy about an officer filming travelers and documents, and 18 were sent to CBP Privacy regarding officers taking photos and scanning wallet contents.

Between April 1 – September 30, 2019, the Department received 142 privacy complaints.

Privacy Complaints Received by DHS Components and the DHS Traveler Redress Inquiry Program *April 1 – September 30, 2019*										
Type	**CBP**	**CISA**	**FEMA**	**ICE**	**TSA**	**USCG**	**USCIS**	**USSS**	**TRIP**	**TOTALS**
Procedure	X		1	1	5		1			**8**
Redress	X									**0**
Operational	X			5	110				19	**134**
Referred	X									**0**
TOTALS	**TBD**[18]	**0**	**1**	**6**	**115**	**0**	**1**	**0**	**19**	**142**

Narrative examples:

FEMA: A former FEMA employee complained that his PII was improperly handled by a member of FEMA's Office of the Chief Counsel. The complaint alleged that PII – to include protected medical information – was emailed to a Yahoo account without proper encryption. The FEMA Privacy Branch investigated the complaint and found credible evidence that the complainant's information was not handled with appropriate safeguards as required by the Privacy Act and DHS policy. However, it was determined that there was no risk of harm as the information was sent to the intended recipients who had a valid and authorized need for the information. Finally, the complaint was forwarded to the Privacy Incident Handling point of contact to be treated as a privacy incident requiring mitigation and remediation.

ICE: As a result of the SSN reduction initiative led by the DHS Privacy Office, an ICE employee contacted ICE Privacy noting his concerns that his name and the last four digits of his SSN appear on forms generated by certain ICE systems. These forms may be circulated to entities outside of DHS, thereby potentially exposing his Sensitive PII. ICE Privacy investigated the employee's concerns, worked with the employee's office, and provided several alternatives to remove employees' SSNs on printed forms. In the interim, ICE Privacy is assessing Human Resources systems and consulting with members of the Chief Human Capital Officer Data Governance Council to replace employee SSNs with an SSN alternative to protect Sensitive PII.

[18] In an effort to employ the most efficient mechanism possible in addressing the concerns of individuals that interact with DHS personnel at Ports of Entry, U.S. Customs and Border Protection is in the process of transitioning to the new CBP Customer Relationship Manager Tool (C2RMT). During the transition period, CBP is unable to access historical data related to the processing of questions, compliments, complaints, comments, and tips from members of the public. Once C2RMT is deployed in full and all historic records have been integrated, CBP will be able to provide examples of complaints that were remediated during the second half of FY2019.

Other complaints cited these issues:

- a survey collecting law enforcement data and PII is hosted on a third-party web site.
- inappropriate interagency distribution of human resources information, including employee personnel records, medical history, and salary.
- collection, retention, and distribution of SSNs for ICE employees.
- unauthorized retention of ICE records after resignation from ICE.

TSA:

- A supervisor kept a log of weekly activities in a shared server for program management purposes and identified the name of an individual who had been issued a letter of counseling. The Privacy Officer notified the Program Director who notified the supervisor of the complaint and directed the deletion of all names of individuals receiving disciplinary action from the shared activities log. The supervisor acknowledged the mistake and provided confirmation that corrective action was taken.
- A passenger complained that her bag had been searched on three recent flights and believed that she was being profiled based on her zip code. The Privacy Office noted that TSA does not receive zip codes as part of the reservations process and does not base any of its screening decisions based on zip codes. TSA is required by law to screen all checked baggage. Many airports have automated in-line baggage screening systems that can screen and clear a bag remotely, resulting in no physical inspection at all. As a result, the amount of time checked baggage is under TSA control is relatively short. On occasion, checked baggage may need to be opened for hand inspection to clear an alarm.

USCIS: A VAWA recipient complained that "state" employees forced them to sign the release of confidential information in exchange for services provided within their state. The complainant used the terms "USCIS employees" when referring to state employees (case workers and desk specialists) they interacted with. USCIS could not comment or address the complaint as it pertained to state or local government actions and not to USCIS/DHS procedures. In addition, after a review, USCIS could not find instances in which the agency disclosed any information about the complainant without their written consent or completed Form a G-28, Notice of Entry of Appearance as Attorney or Accredited Representative.