Department of Homeland Security

Privacy Office

Fiscal Year 2018 Semiannual Report to Congress

For the period April 1 – September 30, 2018

December 20, 2018

Homeland Security

FOREWORD

December 20, 2018

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's Fiscal Year 2018 Semiannual Report to Congress, covering the time period April 1 – September 30, 2018.[1]

Highlights

During the reporting period, the Privacy Office:

- Completed 1,129 privacy reviews, including:
  - 609 Privacy Threshold Analyses;
  - 43 Privacy Impact Assessments; and
  - 12 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,

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

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

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

The Honorable 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 Government Reform

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

Privacy Office
Fiscal Year 2018
Semiannual
Section 803 Report to Congress

Table of Contents

FOREWORD 2
LEGISLATIVE LANGUAGE 6
I. PRIVACY REVIEWS 7
II. ADVICE AND RESPONSES 15
III. TRAINING AND OUTREACH 16
IV. PRIVACY COMPLAINTS AND DISPOSITIONS 20

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 (PCR), 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;
9. Information Technology Acquisition Reviews[11] (ITAR); and
10. Other privacy reviews, such as implementation reviews for information sharing agreements.

[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, 2018

Type of Review	*Number of Reviews*
Privacy Threshold Analyses	609
Privacy Impact Assessments	43
System of Records Notices and associated Privacy Act Exemptions	12
Privacy Act (e)(3) Statements[12]	24
Computer Matching Agreements	0
Data Mining Reports	0
Privacy Compliance Reviews	0
Privacy Reviews of IT and Program Budget Requests[13]	40
Information Technology Acquisition Reviews[14] (ITAR)	401
Other Privacy Reviews	0
Total Reviews	***1,129***

[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] The Chief Information Office 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.
[14] 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 31, 2018, 98 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 43 PIAs: 22 new and 21 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/ALL/PIA-064 Preventing and Combating Serious Crime (PCSC) Agreements - Greece and Italy *(April 3, 2018)*

PCSC Agreements permit the United States and its partner countries to cooperatively exchange biometric and biographic data in the course of preventing and combating serious crimes and terrorist activities. DHS owns and maintains the Automated Biometric Identification System (IDENT), which is responsible for processing automated fingerprint queries to determine if a person of interest encountered by a partner country has also been encountered by DHS. The existing PCSC agreements between DHS and its partners allow for the exchange of information for the purpose of preventing, detecting and investigating serious crimes. The implementing agreements with Greece and Italy further detail how the parties will share information pursuant to the agreement in support of migrant vetting operations. The DHS Privacy Office published this PIA to identify risks and mitigations associated with this information sharing, and to discuss the legal and policy justifications for sharing non-criminal justice data from USCIS with Greece and Italy under the Greece and Italy PCSC Agreements, for purposes of immigration vetting and criminal justice, including border enforcement processes.

DHS/TSA/PIA-049 TSA Office of Inspection Case Management *(July 26, 2018)*

Transportation Security Administration (TSA) Office of Inspection (OOI) conducts covert testing of security screening operations; inspects TSA operations at airports, field offices, and other transportation entities; and investigates employee misconduct and program fraud, and violations of transportation security requirements. OOI's hotline referral and case management systems maintain Personally Identifiable Information (PII): (1) from individuals submitting information to OOI; and (2) on individuals designated as witnesses, victims, complainants, or subjects of an investigation. Since OOI Case Management maintains PII on members of the public, TSA published a PIA to assess the program's privacy impact on individuals, in accordance with Section 208 of the *E-Government Act of 2002* and Section 222 of the *Homeland Security Act of 2002*.

DHS/USCIS/PIA-073 USCIS and CIS Ombudsman Information Sharing *(August 2, 2018)*
The Office of the Citizenship and Immigration Services Ombudsman (CIS Ombudsman), established by Section 452 of the *Homeland Security Act of 2002*, provides independent analysis of problems encountered by individuals and employers who have submitted benefit request filings to USCIS, and proposes changes to mitigate those problems. Sharing information between USCIS and CIS Ombudsman, when there is proper consent, is crucial to fulfilling this statutory mandate. USCIS conducted this PIA to discuss how USCIS provides information to CIS Ombudsman in order to (1) assist individuals and employers with resolving problems with USCIS; (2) identify programmatic areas where individuals and employers have problems in dealing with USCIS; and (3) propose changes to mitigate those problems.

DHS/ALL/PIA-067 Continuous Evaluation (CE) Travel Record Data Service (TRDS) *(August 15, 2018)*
The Travel Record Data Service (TRDS) is a DHS project whereby U.S. Customs and Border Protection (CBP) travel records are shared with the Office of the Director of National Intelligence (ODNI) National Counterintelligence and Security Center (NCSC) Continuous Evaluation System (CES). NCSC provides authorized Executive Branch agencies with TRDS information via the CES to continuously evaluate the suitability of "covered individuals." NCSC then shares relevant CBP traveler information with the covered individual's home agency or authorized Investigative Service Provider to allow that home agency to determine if a security-relevant issue exists. DHS published this PIA to describe the PII within TRDS, and the way in which the data is transferred to the NCSC CES.

DHS/USSS/PIA-023 Applicant Lifecycle Information System (ALIS) *(August 21, 2018)*
United States Secret Service (USSS) Office of Human Resources (HUM) uses the Applicant Lifecycle Information System (ALIS) to support the hiring process for USSS Special Agents (SA), Uniformed Division (UD) Officers, and Administrative, Professional, Technical (APT) personnel. ALIS is a new system that will replace the Clearances, Logistics, Employees, Applicants, and Recruitment (CLEAR) application component of the USSS Human Capital Management System (HCMS). The USSS conducted this PIA because ALIS collects PII from current USSS employees and members of the public.

Updated Privacy Impact Assessments

DHS/CBP/PIA-018(a) Aircraft Systems *(April 6, 2018)*
U.S. Customs and Border Protection (CBP) employs several types of aircraft, including manned helicopters, fixed-wing aircraft, and Unmanned Aircraft Systems (UAS) for border surveillance and law enforcement purposes. These aircraft may be equipped with video, radar, and sensor technologies to assist CBP in patrolling the border, conducting surveillance for law enforcement investigations or tactical operations, or gathering data to assist in disaster relief and emergency response. In addition, the United States Border Patrol (USBP) operates Small Unmanned Aircraft Systems (sUAS) in support of its border security mission. CBP updated this PIA to provide notice of CBP's use of sUAS not addressed in the original PIA, and to assess the privacy impacts of its use of this technology.

DHS/CBP/PIA-022(a) Border Surveillance Systems (BSS) *(August 21, 2018)*
CBP deploys Border Surveillance Systems (BSS) to provide comprehensive situational awareness along the U.S. 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. CBP updated this PIA to assess the 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 the use of commercially available location data to identify activity in designated areas within or near the U.S. border.

DHS/ICE/PIA-020(c) Alien Criminal Response Information Management System (ACRIMe) *(September 28, 2018)*
The Alien Criminal Response Information Management System (ACRIMe) is an information system used by U.S. Immigration and Customs Enforcement (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 original ACRIMe PIA was published on April 22, 2010, and has since been updated on September 29, 2010, and January 24, 2013. ICE updated this PIA again to document several changes: (1) that the ACRIMe Field Module ("ACRIMe Field" or "Field") is being deployed to Enforcement and Removal Operations (ERO) Field Offices across the country; (2) to indicate that the module formerly referred to as the National Crime Information Center (NCIC) Section Module is now called the Wants and Warrants Module; (3) to describe the technical services that ACRIMe uses to query other government databases for relevant information; and (4) to explain that ICE is now using ACRIMe to respond to inquiries submitted by the U.S. Department of Health and Human Services (HHS) regarding the immigration status of potential sponsors of unaccompanied alien children.

DHS/USCIS/PIA-027(d) USCIS Asylum Division *(September 27, 2018)*
The Asylum Division of USCIS adjudicates applications for asylum, benefits pursuant to Section 203 of the Nicaraguan Adjustment and Central American Relief Act (NACARA § 203), withholding of removal under the terms of a settlement agreement reached in a class action, and screening determinations for safe third country, credible fear, and reasonable fear. The Asylum Division historically used the Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS) in support of its mission critical functions. Both systems were originally developed by the former Immigration and Naturalization Service. The Asylum Division is seeking to retire APSS and RAPS and use the Global system, operating in a cloud-based environment, to serve as the primary Information Technology case management system for the administration of affirmative asylum, NACARA § 203, withholding of removal under the terms of a settlement agreement reached in a class action, credible fear, and reasonable cases. USCIS updated this PIA because the Asylum Division uses the new cloud-based Global system and has migrated records containing PII from APSS and RAPS into Global in order to conduct its adjudications.

System of Records Notices

The Department publishes System of Records Notices (SORN) consistent with the requirements outlined in the *Privacy Act of 1974*.[15] 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 the Office of Management and Budget (OMB) and Congress.

As of September 31, 2018, 100 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the Office published 11 SORNs: 4 new and 7 updated, and four Privacy Act rulemakings.

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/ALL-041 External Biometric Records (EBR) System

The External Biometric Records (EBR) System processes and maintains biometric and associated biographic information from non-DHS entities, both foreign and domestic, for law enforcement, national security, immigration screening, border enforcement, intelligence, national defense, and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities. DHS may use and share these external biometric and associated biographic records for these same purposes, as permitted and approved by our partners, if applicable, pursuant to the agreement or arrangement. *(83 Fed. Reg. 17829, April 24, 2018)*

- ***Notice of Proposed Rulemaking***: In this proposed rulemaking, the Department proposed to exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. *(83 Fed. Reg. 17766, April 24, 2018)*

DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System

IBBC assists USCIS with determining an individual's eligibility for an immigration benefit request or other USCIS requests. USCIS collects biographic and biometric data from applicants, petitioners, sponsors, beneficiaries, or other individuals to facilitate three key operational functions: (1) enroll, verify, and manage an individual's identity; (2) conduct criminal and national security background checks; and (3) produce benefit cards/secure documents as a proof of benefit. Also, the purpose of this system is to support data sharing initiatives between DHS Components and other U.S. Government agencies and foreign partners to prevent terrorism, including terrorist travel; prevent serious crime and other threats to national security and public safety; and assist in the administration and enforcement of immigration laws. *(83 Fed. Reg. 36950, July 31, 2018)*

- ***Notice of Proposed Rulemaking***: In this proposed rulemaking, the Department proposed to exempt portions of this system of records from one or more provisions of the Privacy Act

[15] 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.

because of criminal, civil, and administrative enforcement requirements. *(83 Fed. Reg. 36792, July 31, 2018)*

Updated System of Records Notices

DHS/ICE-007 Criminal History and Immigration Verification (CHIVe)

The purposes of the CHIVe system are: (1) to assist in identifying and arresting individuals in the United States who may be subject to removal under the Immigration and Nationality Act, as amended; (2) to respond to inquiries from criminal justice agencies that seek to determine the immigration status of an individual in the context of a criminal justice matter for the purpose of identifying and arresting those who may be subject to removal; (3) to screen individuals to verify or ascertain citizenship or immigration status, immigration history, and criminal history to inform determinations regarding sponsorship of unaccompanied alien children who are in the care and custody of HHS and to identify and arrest those who may be subject to removal; and (4) to inform criminal justice agencies and agencies conducting background checks whether an individual is under investigation and/or wanted by ICE or other criminal justice agencies. *(83 Fed. Reg. 20844, May 8, 2018)*

- ***Notice of Proposed Rulemaking***: In this proposed rulemaking, the Department proposed to rename the system Criminal History and Immigration Verification, and exempt portions of this system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. *(83 Fed. Reg. 20738, May 8, 2018)*

DHS/TSA-001 Transportation Security Enforcement Record System

The Transportation Security Enforcement Record System maintains 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. They may be used, generally, to identify, review, analyze, investigate, and prosecute violations or potential violations of transportation security laws, regulations, and directives, or other laws, as well as to identify and address potential threats to transportation security. They may also be used to record the details of TSA security-related activity, such as passenger or property screening. *(83 Fed. Reg. 43888, August 28, 2018)*

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 did not publish any PCRs during this reporting period. All public PCRs are available on the Privacy Office website, www.dhs.gov/privacy, under Privacy Oversight.

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 on page one.

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

Privacy Policy Initiatives

- The Privacy Office began participating in several intra- and inter-agency working groups and meetings to identify and mitigate privacy concerns that may arise from implementation of Executive Order 13780, "*Protecting the Nation from Foreign Terrorist Entry into the United States,*" and other recent proposals for enhanced screening and vetting measures. Two such initiatives are related to the implementation activities associated with National Security Presidential Memoranda (NSPM) -7 and NSPM-9. See the *2018 Privacy Office Annual Report* for more information.

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

- In the FY 2018 *Appropriations Act* for DHS,[16] Congress provided the Privacy Office with additional funding to ensure information and data released by the Department does not reveal the identity or PII of non-U.S. Persons who may be survivors of domestic violence, sexual assault, stalking, human trafficking, or other crimes. The Privacy Office and the Office for Civil Rights and Civil Liberties (CRCL) developed a process for the two offices to share incidents of unauthorized disclosures, and partner to ensure that incidents are appropriately reviewed, investigated, addressed, and resolved.

Publications

The Privacy Office published the inaugural report to Congress required by the *Social Security Number Fraud Prevention Act of 2017* to document the Privacy Office's multi-year plan to reduce the collection, use, and mailing of Social Security numbers at DHS.

[16] The Consolidated Appropriations Act, 2018 (Pub.L. 115–141).

III. Training and Outreach

Mandatory Online Training

139,224 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.

3,781 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

3,764 DHS personnel attended instructor-led privacy training courses, including the following for which the Privacy Office either sponsored or provided a trainer:

- ***New Employee Training***: 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 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.
- ***FOIA Training***: This periodic training is tailored to FOIA staff throughout the agency responsible for processing FOIA requests.
- ***Nationwide Suspicious Activity Reporting Initiative*:** The Privacy Office provides training in privacy principles to Suspicious Activity Reporting analysts.
- ***DHS 201 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.
- ***DHS Security Specialist Course*:** The Privacy Office provides privacy training every six weeks to participants of this week-long training program, who represent multiple agencies.
- ***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.
- ***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.
- ***Fusion Center Training:*** Privacy Office staff helped plan and participated in a Privacy/Civil Rights and Civil Liberties (P/CRCL) workshop for fusion center privacy officers and senior personnel in Lincoln, Nebraska on September 26 and 27. Presentations included: Roles and Responsibilities for P/CRCL Officers; Emerging Technologies (License Plate Readers, Facial Recognition, Body Worn Camera, 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 Guam, Florida, Vermont, Washington, and many locations in between attended. In August, Privacy Office staff provided introductory privacy training to 16 new fusion center directors and assistant directors.

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***: On March 27 - 28, 2018, in Washington, DC, the Chief Privacy Officer (CPO) interviewed CBP's Deputy Assistant Commissioner on border security and privacy, and the Deputy CPO participated on a panel, *How to Get a Privacy Job in the Federal Government*.
- ***NSPM-9/National Vetting Center***: On April 5, 2018, the National Vetting Governance Board's Privacy, Civil Liberties, and Civil Rights Working Group, of which the CPO is a co-chair, held a listening session attended by civil liberties, civil rights, and privacy advocacy organizations. The purpose was to hear questions and concerns about NSPM-9 and the National Vetting Center while plans for implementation are still being developed. The meeting was attended by the Senior Agency Officials for Privacy from the Departments of State, Defense, and Justice, the Central Intelligence Agency, the Federal Bureau of Investigation, and the Office of the Director for National Intelligence. The government representatives gave an overview of NSPM-9, and addressed questions about its scope and possible application to various immigration and border security programs.
- ***DHS Information Law Symposium***: On May 1, 2018, in Washington, DC, the CPO gave the key address on *How Transparency and Openness Help to Facilitate Our Mission.*
- ***Legal and Policy Seminar sponsored by Thompson Hine***: On May 8, 2018, in Washington, DC, the CPO gave the keynote address on How to Establish an Effective Privacy Program.
- ***Department of Justice Privacy Training***: On May 15, 2018, in Washington, DC, the CPO participated in a panel discussion on international privacy issues, including the U.S. – European Union (EU) Passenger Name Record (PNR) Agreement, the National Vetting Center, and the European Union's General Data Protection Regulation (GDPR) impact on DHS.
- ***Meeting of the Data Privacy and Integrity Advisory Committee's (DPIAC) Cyber Subcommittee***: On May 22, 2018, the National Protection and Programs Directorate (NPPD) Office of Privacy hosted a meeting with the leadership of the NPPD Office of Cybersecurity and Communications (CS&C) to provide an update on recent privacy projects and initiatives at CS&C. The meeting also included an open discussion of the potential effects of the GDPR on the NPPD cyber mission.
- ***American Society of Access Professionals Eleventh National Training Conference***: In July 2018, in Arlington, VA, the CPO gave a speech on how DHS is improving FOIA responsiveness and performance to meet increasing demand, and the Deputy CPO, along with the Department of Transportation's CPO, co-presented scenario-based privacy challenges.
- ***Meeting of the DPIAC Policy Subcommittee***: On July 10, 2018, members of the DPIAC's Policy Subcommittee, along with officials from the DHS Privacy Office and CBP's Offices of Privacy and Field Operations, toured biometric entry and exit operations at Orlando International Airport to observe general passenger processing operations, including pilot entry and exit programs. Attendees were briefed on data collection, uses, and sharing associated with the entry processing of arriving visitors, as well as a pilot program in which CBP has collaborated with British Airways to use biometric data (facial images) to verify a traveler's identity and process them for exit. The pilot utilizes an e-gate in the boarding area of the departure terminal, and allows passengers to board their flight without presenting any travel documentation or a boarding pass. Back-end

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

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

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.

Federal Emergency Management Agency (FEMA)

- Conducted in-person Privacy 101 (general privacy awareness) training to several FEMA Components and offices, to include the Office of External Affairs, Federal Insurance and Mitigation Administration, Office of Response and Recovery, and Office of the Chief Human Capital Officer.
- Conducted privacy training for the disaster workforce at the Puerto Rico Joint Field Office (JFO), and provided a "train the trainer" program to ensure that FEMA workforce at field offices and disaster recovery centers (DRCs) also received privacy training.
- Held a PIA Writing Instructional Training class for FEMA system owners and information system security officers (ISSOs) as part of the "FISMA surge effort" to improve the quality and analysis of compliance documentation, and minimize the time needed to get it approved.
- Provided privacy awareness training to individuals as direct remediation for privacy incidents.

National Protection and Programs Directorate (NPPD)

- Provided a Privacy Briefing during New Employee Orientation to 176 new NPPD employees from all sub-components.
- Provided an executive-level privacy briefing to one new Senior Executive Service employee.
- Provided Component privacy training to 52 employees and contractors for the Personnel Security Division at the Federal Protective Service (FPS).
- Provided a role-based privacy briefing and privacy guidance during an Infrastructure Protection (IP) All-Hands meeting with the IP Field Operations Branch and the Regional Chemical Security Inspector Supervisors.
- Provided the privacy portion of a joint *Paperwork Reduction Act and Privacy* briefing to members of the Office of Infrastructure Protection (IP) Infrastructure Security and Compliance Division.
- Presented at a one-hour webinar on the changing landscape of privacy and how it effects information security strategies for protecting information residing on systems and networks.
- Provided role based privacy training to 75 participants throughout NPPD in a "Lunch and Learn" webinar entitled *Privacy Incident Reporting Webinar*.
- Participated in the Federal Identity Summit in Tampa, Florida. OBIM Privacy spoke with vendors, academia, and government representatives about OBIM's biometric services and privacy compliance program.
- Participated in the Office of Infrastructure Protection's IP Workforce Mission Day on April 17, 2018. The analysts staffed a booth at the event, and provided privacy information/guidance, answered privacy related questions and provided take-aways to those who stopped by the booth, including NPPD and DHS privacy policies, factsheets, and privacy incident reporting cards.

- Published five privacy related articles in NPPD's weekly newsletter, entitled *NPPD Vision,* and two issues (June and September) of the quarterly newsletter, entitled the *NPPD Privacy Update.* The newsletter is distributed NPPD-wide and posted on the NPPD Office of Privacy internal intranet page.

United States Citizenship and Immigration Services (USCIS)

- Continue to work with the Office of Human Capital and Training/ Instructional Design and Development Branch to modernize the privacy awareness computer-based training that will be added to the PALMS training platform along with a video from the USCIS Privacy Officer.
- Conducted six Social Media Privacy Training sessions for Fraud Detection and National Security Directorate employees who have been approved to use social media for operational use.
- Promoted the annual Privacy Tips Campaign in the USCIS Today (Spotlight) and via digital signage.
- Launched new training videos in which the Privacy Officer promotes privacy awareness at headquarters and in the Service Center Operations.
- Conducted a *Lunch & Learn Privacy – Do You Have a Choice?* seminar that included a briefing from the Office of Management and Budget along with a Privacy Awareness training to over 350 USCIS employees.

United States Coast Guard (USCG)

- Trained 120 new employees on the importance of protecting personal information.

United States Immigration and Customs Enforcement (ICE)

- Provided a Privacy Briefing during New Employee Orientation to 206 new ICE employees.
- Trained ICE Homeland Security Investigations, Office of Intelligence on disclosures under the Privacy Act, the properly handling of sensitive PII, and privacy incident response and prevention.
- Provided *ICE Fundamentals of Mission Support* training to 39 employees, addressing general privacy and records management concepts, as well as an overview of FOIA requests and responses.
- Trained 11 ISSOs on privacy and information security requirements.

United States Secret Service (USSS)

- Trained 5,021 employees and contractors on mandatory annual privacy awareness training.
- Trained 2,866 employees on the "Operational Use of Social Media" training.

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]

Table II: Type and Disposition of Privacy Complaints Received This Reporting Period

Complaint Type	Complaints received during the reporting period	Complaint Disposition		
		Closed, Responsive Action Taken[18]	In Progress (Current Period)	In Progress (Prior Periods)
Process & Procedure	736	723	13	0
Redress	5,153	5,829	172	0
Operational	2,681	2,627	57	0
Referred	439	432	7	0
Total	**9,009**	**9,611**	**249**	**0**

.

DHS separates complaints into four categories:

1. ***Process and Procedure****:* Issues concerning process and procedure, such as consent, or appropriate notice at the time of collection.
    a. *Example*: An individual submits a complaint that alleges a program violates privacy by collecting Social Security numbers without providing proper notice.
2. ***Redress***: Issues concerning appropriate access and/or correction of PII, and appropriate redress of such issues.
    a. *Example*: Misidentifications during a credentialing process or during traveler inspection at the border or screening at airports.[19]
3. ***Operational***: Issues related to general privacy concerns, and concerns not related to transparency or redress.
    a. *Example:* An employee's health information was disclosed to a non-supervisor.
4. ***Referred****:* The Privacy Office or another DHS Component determined that the complaint would be more appropriately handled by another federal agency or entity, and referred the complaint to the appropriate organization. This category does not include internal referrals within DHS. The referral category both serves as a category of complaints and represents

[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.

[18] These totals include complaints opened and closed during this reporting period, and complaints opened in prior reporting periods but closed during this reporting period.

[19] This category excludes FOIA and Privacy Act requests for access, which are reported annually in the Annual FOIA Report, and Privacy Act Amendment requests, which are reported annually in the DHS Privacy Office Annual Report to Congress.

responsive action taken by the Department, unless a complaint must first be resolved with the external entity.

a. *Example*: An individual has a question about his or her driver's license or Social Security number, which the Privacy Office refers to the proper agency.

DHS Components and the Privacy Office report disposition of complaints in one of the two following categories:

1. *Closed, Responsive Action Taken*: The Privacy Office or another DHS Component reviewed the complaint and took responsive action. For example, an individual may provide additional information to distinguish himself from another individual. In some cases, acknowledgement of the complaint serves as the responsive action taken. This category may include responsive action taken on a complaint received from a prior reporting period.

2. *In Progress*: The Privacy Office or another DHS Component is reviewing the complaint to determine the appropriate action and/or response. This category identifies in-progress complaints from both the current and prior reporting periods.

The following are examples of complaints received during this reporting period, along with their disposition:

Transportation Security Administration (TSA)

COMPLAINT:
An employee complained to TSA Privacy that their airport coordination center had begun to use a third party website and mapping system to "geo-tag" the home addresses of Transportation Security Officers for use during emergency operations and in response to natural disasters. TSA Privacy worked with the airport's leadership to ensure that access to the website was limited to users with an official need-to-know.