
# Department of Homeland Security

Privacy Office

Fiscal Year 2017 Semiannual Report to Congress

*For the period October 1, 2016 – March 31, 2017*

*June 29, 2017*

Homeland Security

# FOREWORD

*June 29, 2017*

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's *Fiscal Year 2016 Semiannual Report to Congress,* covering the time period October 1, 2016 – March 31, 2017.[1]

## Highlights

During the reporting period, the Privacy Office:

- Completed 830 Privacy Reviews, including 496 Privacy Threshold Analyses, 25 Privacy Impact Assessments, 13 System of Records Notices, and two Privacy Compliance Reviews.
- Published the *2016 Privacy Office Annual Report to Congress*.
- Issued two new Privacy Policy Instructions on Privacy Compliance Reviews and DHS Component Privacy Officers.
- Received guidance from our Federal Advisory Committee, the Data Privacy and Integrity Advisory Committee, on best practices for notifying individuals impacted by a large-scale data breach.

## About the Privacy Office

The *Homeland Security Act of 2002* charges the DHS Chief Privacy Officer with primary responsibility for ensuring that privacy considerations and 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 Privacy Office at 202-343-1717 or privacy@dhs.gov, 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] Most DHS Components have a Privacy Officer or Privacy Point of Contact. Contact information can be found here: http://www.dhs.gov/privacy-office-contacts.

Sincerely,

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

Pursuant to congressional notification requirements, the Privacy Office provides this report to the following Members of Congress:

**The Honorable Michael Pence**
President, U.S. Senate

**The Honorable Paul D. Ryan**
Speaker, U.S. House of Representatives

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

**The Honorable Claire McCaskill**
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

**The Honorable Charles Grassley**
Chairman, U.S. Senate Committee on the Judiciary

**The Honorable Dianne Feinstein**
Ranking Member, U.S. Senate Committee on the Judiciary

**The Honorable Richard Burr**
Chairman, U.S. Senate Select Committee on Intelligence

**The Honorable Mark Warner**
Vice Chairman, U.S. Senate Select Committee on Intelligence

**The Honorable Michael McCaul**
Chairman, U.S. House of Representatives Committee on Homeland Security

**The Honorable Bennie G. Thompson**
Ranking Member, U.S. House of Representatives Committee on Homeland Security

**The Honorable Jason Chaffetz**
Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

**The Honorable Elijah Cummings**
Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

**The Honorable Bob Goodlatte**
Chairman, U.S. House of Representatives Committee on the Judiciary

**The Honorable John Conyers, Jr**.
Ranking Member, U.S. House of Representatives Committee on the Judiciary

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

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

# Privacy Office
# Fiscal Year 2017
# Semiannual
# Section 803 Report to Congress

## Table of Contents

# LEGISLATIVE LANGUAGE

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

> "(f) Periodic Reports-
>
> (1) In General –
>
> The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than semiannually, submit a report on the activities of such officers—
>
> (A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;
>
> (ii) to the head of such department, agency, or element; and
>
> (iii) to the Privacy and Civil Liberties Oversight Board; and
>
> (B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.
>
> (2) Contents –
>
> Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—
>
> (A) information on the number and types of reviews undertaken;
>
> (B) the type of advice provided and the response given to such advice;
>
> (C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and
>
> (D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer."

[3] 42 U.S.C. § 2000ee-1(f).

# I. PRIVACY REVIEWS

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

1. Privacy Threshold Analyses, which are the DHS foundational mechanism for reviewing IT systems, programs, and other activities for privacy protection issues to determine whether a more comprehensive analysis is necessary, either through, e.g., by completing a Privacy Impact Assessment or a Systems of Records Notice;
2. Privacy Impact Assessments, as required under the *E-Government Act of 2002*,[4] the *Homeland Security Act of 2002*,[5] and DHS policy;
3. System of Records Notices, as required under the *Privacy Act of 1974*, and any associated Final Rules for Privacy Act exemptions;[6]
4. Privacy Act Statements, as required under the Privacy Act,[7] to provide notice to individuals at the point of collection;
5. Computer Matching Agreements, as required under the Privacy Act;[8]
6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*;[9]
7. Privacy Compliance Reviews, per the authority granted to the Chief Privacy Officer by the *Homeland Security Act of 2002*;[10]
8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) Exhibit 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board;
9. Information Technology Acquisition Reviews[11] (ITAR); and
10. Other privacy reviews, such as implementation reviews for public-facing 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 exercises 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**<br>**Privacy Reviews Completed:**<br>***October 1, 2016 – March 31, 2017*** | |
|---|---|
| ***Type of Review*** | ***Number of Reviews*** |
| Privacy Threshold Analyses | 496 |
| Privacy Impact Assessments | 25 |
| System of Records Notices and associated Privacy Act Exemptions | 13 |
| Privacy Act (e)(3) Statements | 10 |
| Computer Matching Agreements | 4 |
| Data Mining Reports | 0 |
| Privacy Compliance Reviews | 2 |
| Privacy Reviews of IT and Program Budget Requests | 99 |
| Information Technology Acquisition Reviews[12] (ITAR) | 181 |
| Other Privacy Reviews | 0 |
| ***Total Reviews*** | ***830*** |

[12] The DHS Privacy Office initiated ITAR reviews in January 2016.

## *Privacy Impact Assessments*

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

As of March 31, 2017, 94 percent of the Department's FISMA systems that require a PIA had an applicable PIA. During the reporting period, the Office published 25 PIAs: 13 new and 12 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-058 DHS Access Lifecycle Management *(January 24, 2017)*
The Access Lifecycle Management (ALM) is the technology and business process that manages the identities and access rights of DHS employees and contractors, ensuring that they only have access to approved systems and applications. DHS published this PIA because ALM uses, stores, and disseminates the PII of DHS employees and contractors in order to manage their accounts and identities.

DHS/USCIS/PIA-064 myUSCIS *(December 14, 2016)*
The U.S. Citizenship and Immigration Services (USCIS) launched myUSCIS, an online platform that provides customers additional digital services to interact with USCIS. The purpose of myUSCIS is to offer online customers a wider range of USCIS services. USCIS is implementing myUSCIS features in a phased approach. This initial PIA and the attached appendices discuss and evaluate the privacy risks and mitigations associated with the collection, use, and maintenance of PII in myUSCIS and its digital services. USCIS will update the appendices of the PIA as subsequent digital services and functionalities are added.

DHS/ICE/PIA-047 Department of Homeland Security – Victim Information and Notification Exchange (DHS-VINE) *(January 10, 2017)*
The DHS Victim Information and Notification Exchange (DHS-VINE) is a new system that DHS U.S. Immigration and Customs Enforcement (ICE) Enforcement and Removal Operations (ERO) established to automatically notify certain individuals about changes to a particular alien's custodial status with ICE. These particular aliens, referred to in this PIA as "aliens," include those who have been charged with a crime, and those convicted of a crime, so long as a crime victim or victim advocate has registered with DHS-VINE to be notified upon change to the alien's custodial status with ICE. This PIA details the protections that are in place for the PII pertaining to eligible registrants as well as the aliens that DHS-VINE collects, uses, and maintains.

DHS/ALL/PIA-059 DHS Employee Collaboration Tools *(February 07, 2017)*
DHS employs various cloud-based services and employee collaboration tools to promote efficiency and improve content management and employee communication across the enterprise. DHS cloud-based services and tools are used by the Department and departmental programs that do not have other content tracking systems to more effectively and efficiently manage the receipt, creation, assignment, tracking, and storage of agency matters. DHS conducted this PIA because cloud-based content management solutions and employee collaboration tools collect, use, store, and disseminate PII and Sensitive PII. This PIA replaces two previous PIAs: DHS/ALL/PIA-023 DHS IdeaFactory (January 21, 2010), and DHS/ALL/PIA-037 DHS SharePoint and Collaboration Sites (March 22, 2011).

DHS/CBP/PIA-038 Cornerstone (*February 27, 2017*)
U.S. Customs and Border Protection (CBP) created the Cornerstone information management system to automate and manage the background investigation (BI) process for CBP employees, contractors, and applicants. Cornerstone facilitates the BI process by retrieving, compiling, and distributing information between several information systems during the BI process. CBP conducted this PIA because Cornerstone collects and maintains PII about employees, applicants, contractors, and members of the public.

## Updated Privacy Impact Assessments

DHS/USCIS/PIA-007(b) Domestically Filed Intercountry Adoptions Applications and Petitions *(November 02, 2016)*
The USCIS Adoption Case Management System (ACMS) module under the National Processing Workflow Repository (NPWR) serves as the case-management system for the domestically-filed intercountry adoption process. ACMS is used by the USCIS National Benefits Center (NBC) to facilitate the effective and efficient processing of domestic intercountry adoption-related applications and petitions. ACMS replaced USCIS's existing intercountry adoption case management system, the Secure Information Management Service. USCIS conducted this PIA because ACMS collects, uses, and disseminates PII. This PIA replaces DHS/USCIS/PIA-007 USCIS Secure Information Management Service (SIMS) Pilot and Inter-country Adoptions and DHS/USCIS/PIA-007(a) Secure Information Management Service (SIMS) Pilot with Inter-Country Adoptions Update.

DHS/USCG/PIA-002(d) Biometrics at Sea System (BASS) *(December 06, 2016)*
As the United States' primary maritime law enforcement agency, the U.S. Coast Guard (USCG or Coast Guard) enforces United States immigration statutes and regulations at ports and at sea. USCG implemented the Biometrics At Sea System (BASS) on 23 of its cutters in the District 7 Area of Responsibility (AOR) to screen individuals attempting to enter the United States illegally via maritime routes. USCG uses BASS to collect and send biometric information to DHS's Automated Biometric Identification System (IDENT), a repository of biometric and associated biographic data used for, among other purposes, national security, law enforcement, and immigration and border management. USCG updated this PIA to modernize its biometric submission and response architecture, and to mitigate risks associated with the processes to expand the collection, use, and maintenance of biometrics collected from individuals interdicted by the Coast Guard.

DHS/CBP/PIA-025(b) 1-to-1 Facial Comparison Project *(October 18, 2016)*
U.S. Customs and Border Protection (CBP) updated the PIA for the 1-to-1 Facial Comparison Project due to a change in the retention of facial images of travelers presenting themselves at the border for customs and immigration inspection. CBP uses facial comparison technology to assist CBP Officers in determining whether an individual presenting a valid electronic passport, or "e-Passport," is the true owner of that document. This PIA update documents CBP's change in procedures to retain select facial images taken during primary inspection, and all facial images taken during secondary inspection.

DHS/CBP/PIA-006(e) Automated Targeting System *(January 13, 2017)*
CBP operates the Automated Targeting System (ATS), a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. CBP updated this PIA to notify the public about ATS's user interface enhancements for passenger vetting (known as Unified Passenger or UPAX), the use of ATS for vetting new populations, vetting of master crew member list and master non-crew member list data collected under 19 CFR.122.49c, and several new information sharing initiatives, including between the Transportation Security Administration (TSA) and CBP to enhance the identification of possible threats and to assist in securing the border and transportation security.

## *System of Records Notices*

The Department publishes System of Records Notices (SORN) consistent with the requirements outlined in the *Privacy Act of 1974*.[13] The Department conducts biennial reviews of SORNs to ensure that they conform to and comply with the standards outlined in the Privacy Act. If no update is required, the original SORN remains in effect.

As of March 31, 2017, 99 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the Office published 8 SORNs: 3 new and 5 updated. DHS also published five Privacy Act rulemakings: four Notices of Proposed Rulemakings and one Final Rule.

All DHS SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act Exemptions 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/USCG-031 USCG Law Enforcement (ULE)
This system of records allows the Coast Guard to collect and maintain records related to maritime law enforcement, marine environmental protection, and the determinations supporting enforcement action taken by the Coast Guard. Additionally, DHS issued a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act. This newly established system is included in DHS's inventory of record systems. *(81 Fed. Reg. 88697, December 08, 2016)*

[13] 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.

- *Notice of Proposed Rulemaking*: DHS gave concurrent notice of a newly established system of records pursuant to the Privacy Act for the "Coast Guard-031 USCG Law Enforcement (ULE) System of Records" and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. *(81 Fed. Reg. 88635, December 08, 2016)*

DHS/CBP-023 Border Patrol Enforcement Records (BPER)

This system of records contains information CBP collects and maintains to secure the U.S. border between the Ports of Entry (POE), furthering its enforcement and immigration mission. CBP issued this new system of records to claim ownership of records created as a result of CBP interactions between the POE. CBP inputs non-intelligence information it collects as a result of these interactions into its E3 Portal. CBP also collects and maintains information related to camera and sensor alerts in its Intelligent Computer Assisted Detection (ICAD) database. This system of records applies to the categories of information input and maintained in these systems, which includes biographic, biometric, geolocation imagery and coordinates, and other enforcement and detention data associated with encounters, investigations, border violence, seized property in relation to an apprehension, inspections, prosecutions, and custody operations of CBP between the POE for law enforcement, immigration, or border security purposes. *(81 Fed. Reg. 72601, October 20, 2016)*

- *Notice of Proposed Rulemaking*: DHS gave concurrent notice of a newly established system of records pursuant to the Privacy Act for the "CBP-023 Border Patrol Enforcement Records (BPER) System of Records," and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. *(81 Fed. Reg. 72551, October 20, 2016)*

## Updated System of Records Notices

DHS/USCIS-007 Benefit Information System

USCIS collects, uses, and maintains the Benefit Information System records to administer immigrant or nonimmigrant benefit requests, hereinafter collectively referred to as "benefit requests," to process and adjudicate all benefit requests submitted for naturalization, lawful permanent residence, asylum, refugee status, and other immigrant and nonimmigrant benefits in accordance with U.S. immigration law. USCIS also uses the Benefit Information System to support national security by preventing individuals from fraudulently obtaining immigration benefits, and by denying benefit requests submitted by individuals who pose national security or public safety threats. USCIS updated this system of records to: (1) update the system location to include international offices and replicated copies on unclassified and classified networks; (2) update the category of individuals to include interpreters, preparers, physicians, and sponsors; (3) expand the categories of records to clarify the data elements that USCIS collects from benefit requestors, beneficiaries, and family members', benefit sponsors; representatives; preparers and interpreters; and physicians; (4) separate routine use (N) into two separate routine uses (i.e., (N), (O)) to provide clarity on information sharing with federal, state, tribal, or local government agencies and foreign government agencies for the repayment of loans; (5) update routine uses (W), (X), (Y), and (Z) to permit the sharing of information pursuant to a Computer Matching Agreement or other agreement, with the Department of Labor, with the public during the course of naturalization ceremonies, and with the Department of Treasury, respectively; (6) update retention schedules for each record type; (7) expand data elements used to retrieve records from the elements listed or a combination thereof; (8) update sources of records to include interpreters,

preparers, and physicians; and (9) expand the system classification to provide notice that Benefit Information System records may be stored on both DHS unclassified and classified networks to allow for analysis and vetting consistent with existing USCIS authorities and purposes and this published notice. Additionally, this notice included non-substantive changes to simplify the formatting and text of the previously published notice. *(81 Fed. Reg. 72069, October 19, 2016)*

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records
ICE collects, uses, and maintains ENFORCE to support the identification, apprehension, and removal of individuals unlawfully entering or present in the United States in violation of the Immigration and Nationality Act, including fugitive aliens. ICE also uses ENFORCE to support the identification and arrest of individuals (both citizens and non-citizens) who commit violations of federal criminal laws enforced by DHS. This system of records was created from a previously issued system of records, DHS/ICE 011-Immigration and Enforcement Operational Records (ENFORCE), *80 Fed Reg 24269, April 30, 2015.* ICE updated this system of records to: change the system of records name to "DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER)" System of Records; update and reorganize the categories of individuals for clarity; expand the categories of records, to include recordings of detainee telephone calls and information about these calls, as well as information related to detainees' accounts for telephone or commissary services in a detention facility; update the system manager; clarify system location; and add twenty-five routine uses and modify twenty routine uses to describe how the Department may share information from this system. Additionally, this notice included non-substantive changes to simplify the formatting and text of the previously published notice. *(81 Fed. Reg. 72080, October 19, 2016)*

## *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 Privacy Impact Assessments (PIA), System of Records Notices (SORN) 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.

Please consult our Standard Operating Procedure for PCRs, completed in November 2016.

The 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.

Privacy Compliance Review of the Analytical Framework for Intelligence (AFI) (*December 2016*)
This is the second PCR on AFI. The DHS Privacy Office found that CBP continues to operate and manage AFI with privacy-protective objectives, and with sensitivity to privacy and data aggregation risks. Of the 16 recommendations made in the 2014 PCR, the DHS Privacy Office notes that CBP fully implemented ten, and is in the process of implementing the remaining six. The DHS Privacy Office strongly encourages full implementation of the 2014 recommendations, and additionally recommends that CBP implement an additional eight recommendations to continue to improve its ability to demonstrate compliance with privacy requirements.

Privacy Compliance Review of the Southwest Border Pedestrian Exit Field Test (*January 2017*)
CBP conducted the Southwest Border Pedestrian Exit Field Test (Test) to determine whether the collection of biometric information, including facial and iris images, from visitors exiting the United States enhances CBP exit operations with acceptable impacts to the public's travel experience and border processing times. Due to the novel technologies and heightened privacy risks involved with the collection of biometrics, particularly with untested biometric modalities, the Test's PIA required the DHS Privacy Office to conduct a Privacy Compliance Review (PCR) at the conclusion of the Test. This PCR was designed to evaluate how the information collected during the Test was used, retained, and destroyed. In keeping with the Test's goals of providing an operational feasibility assessment for potential future deployment, the recommendations of this PCR are also intended to provide CBP with best practices and an initial privacy compliance framework for potential future deployments of biometric collection technologies and processes.

# 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 *2016 Privacy Office Annual Report* cited on page one.

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

## *Privacy Policy*

The DHS Privacy Office issued two new Privacy Policy Instructions during the reporting period:

- DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews (*January 2017*) This Instruction implements DHS Directive 047-01, "Privacy Policy and Compliance," with regard to the DHS Component Head's responsibility to assist the Chief Privacy Officer in reviewing Component activities to ensure that privacy protections are fully integrated into Component operations.

- DHS Privacy Policy Instruction 047-01-005 for Component Privacy Officers (*February 2017)* This Instruction requires the DHS Components to appoint a Privacy Officer within each Component to oversee privacy compliance, policy, and oversight activities in coordination with the Chief Privacy Officer.

## *Information Sharing*

The Privacy Office collaborates with Component privacy offices, the DHS Office of Intelligence and Analysis (I&A), CRCL, the Office of Policy (PLCY), DHS Component data stewards, and external information sharing partners to ensure that the Department executes its information sharing programs in a privacy-protective manner.

Through these collaborative relationships, the Privacy Office:

- provides leadership and privacy subject-matter expertise in DHS's ongoing evaluation of its information sharing with the Intelligence Community (IC).
    - As part of DHS's DARC, the Office incorporates privacy best practices, such as protections related to transparency, oversight, and redress, into Information Sharing and Access Agreements (ISAA) with the IC.
    - The Privacy Office continues to participate in quarterly reviews of the National Counterterrorism Center's (NCTC) use of DHS data, including its application of baseline safeguards.
- advises on domestic and international information sharing agreements to ensure consistency with U.S. privacy law and DHS privacy policy, particularly on sharing that occurs through biometric-based query and response, and
- maintains a leadership role in DHS's internal information sharing and management governance processes.

## *Policy Recommendations*

In September 2015, the former Chief Privacy Officer tasked the Privacy Office's Federal Advisory Committee, the Data Privacy and Integrity Advisory Committee (DPIAC),[14] to provide written guidance on best practices for notifying individuals impacted by a large-scale data breach.

In response, on February 21, 2017, the DPIAC issued *Report 2017-01, Best Practices for Notifying Affected Individuals of a Large-Scale Data Breach*. The report is structured in four sections, each of which contains insight and recommendations for DHS to consider:

1. Making the decision to notify the affected individuals
2. Preparing and delivering the notice
3. Concerns about over-notification
4. Providing additional support for affected individuals

[14] The DPIAC provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to personally identifiable information, as well as data integrity and other privacy-related matters. The DPIAC was established by the Secretary of Homeland Security under the authority of 6 U.S.C. § 451 and operates in accordance with the provisions of the Federal Advisory Committee Act (FACA) (5 U.S.C. App). More information on the DPIAC can be found here: https://www.dhs.gov/privacy-advisory-committee.

# III. Training and Outreach

## *Mandatory Online Training*

109,056 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.

2,874 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*

4,471 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.

## 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.

- ***Federal Privacy Summit*** – On November 10, 2016, in Washington, DC, the Federal Privacy Council hosted a one-day workshop that convened privacy, technology, budget, procurement, human resources, public affairs, congressional affairs, and intergovernmental affairs staff from many federal agencies to discuss privacy and security. Subject matter experts, including the Acting Chief Privacy Office (CPO), shared best practices for protecting privacy, and ways to improve collaboration across the enterprise. Marc Groman from the Office of Management and Budget (OMB) gave the keynote address.
- ***FedScoop's Federal Executive Leadership Roundtable on Emerging Technology*** – On December 1, 2016, in Washington, DC, the Acting CPO joined other government panelists to discuss best practices on emerging technology in the public sector.
- ***The International Association of Privacy Professionals Practical Privacy Series*** – On December 8, 2016, in Washington, DC, the Acting CPO hosted a one-day workshop on technology issues facing public sector privacy professionals. Marc Groman from the OMB gave the keynote address.
- ***U.S. Department of Health and Human Services (HHS) Data Privacy Day Workshop*** – On January 26, 2017, in Washington, DC, the HHS Privacy Director moderated a panel of privacy experts to discuss the past, present, and future of privacy in the Federal Government.
- ***Data Privacy and Integrity Advisory Committee Meeting*** – On February 21, 2017, the Privacy Office hosted a virtual public meeting of the Data Privacy and Integrity Advisory Committee (DPIAC). Members deliberated, voted on, and subsequently issued their *Report 2017-01, Best Practices for Notifying Affected Individuals of a Large-Scale Data Breach*.

## 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)

- Supported FEMA's Workplace Transformation initiative by conducting privacy training and site risk analysis in the National Capital Region (NCR), and in targeted Regional Offices and field sites to reinforce best practices for securing PII during office relocations and disaster operations.
- Initiated expansion of the Privacy Office footprint into disaster operations offices and sites by having a Privacy Point of Contact at each disaster site to provide "just in time" privacy training, disseminate privacy resource materials, and conduct privacy compliance site assessments. The goal is to embed and improve privacy protection and oversight in FEMA disaster operations environments and reduce privacy incidents.
- Provided a privacy resource packet (privacy fact sheets, privacy posters, and best practice materials) to the Office of Response and Recovery, Individual Assistance Division, for inclusion in each Disaster Recovery Office set-up kit. The FEMA Privacy Office also disseminated these materials across the enterprise to enhance PII protection as well as privacy incident reporting and mitigation.
- Served on the agency's Intranet Governance Working Group to establish governance on FEMA's use of SharePoint, specifically with respect to safeguarding PII.

- Served on the agency's Information Technology Acquisition Review board to address privacy risks and ensure appropriate cyber hygiene clauses are incorporated into FEMA's contracts.
- Continued to focus on ensuring privacy compliance of FEMA's systems, programs, projects, and initiatives through development, review, and approval of Privacy Threshold Analyses, Privacy Impact Assessments, Systems of Records of Notices, Privacy Act Section e(3) Statements, and Computer Matching Agreements. Additionally, training and awareness continued to be a priority in as much as the FEMA Privacy Office continued to provide specialized privacy training to information management professionals; and remedial training as a result of privacy incidents or potential privacy risks.

## National Protection and Programs Directorate (NPPD)

- NPPD Office of Privacy provided a Privacy Briefing during New Employee Orientation to a total of 216 new NPPD employees from all subcomponents.
- NPPD Deputy Director, Privacy and a Senior Privacy Analyst presented at an International Association of Privacy Professionals (IAPP) KnowledgeNet event on "Designing Cyber Information Sharing with Privacy in Mind – Post Cybersecurity Information Sharing Act (CISA). The presentation focused on the privacy protections in CISA and how NPPD built privacy into their Automated Indicator Sharing (AIS) initiative.
- NPPD Deputy Director, Privacy participated on a Cybersecurity Information Sharing panel at the Department of Justice Privacy Forum.
- NPPD Senior Privacy Analyst provided Privacy 101 training for the Human Capital and Security All Hands Training with a total of 37 attendees.
- NPPD Director, Privacy provided IT Security for Privacy Professionals training for week six of the Federal Privacy Council's Boot Camp.
- *Chief Security Officer Online* published a blog co-authored by an NPPD Director, entitled, "*Putting the Privacy into Cybersecurity at DHS*."
- NPPD Privacy Analyst provided Privacy & Acquisitions training during the Information Technology Acquisition Review (ITAR) Submitter Training as the privacy representative to 43 employees/contractors. The training was targeted for new submitters in the ITAR process or refresher training for current submitters.
- NPPD Office of Biometric Identity Management (OBIM) Section Chief for Privacy, Policy, and FOIA participated in a panel discussion on the *Perceptions of Privacy* held by the International Biometric Institute. The panel engaged in a focused discussion on public perceptions and attitudes towards privacy impact biometric adoption and international information sharing.
- NPPD Office of Privacy published three privacy-related articles in NPPD's weekly newsletter, *NPPD Vision*, which is distributed NPPD-wide. The articles covered subjects such as doxxing and Data Privacy Day.
- NPPD Office of Privacy published two issues (December and March) of their quarterly newsletter, entitled the *NPPD Privacy Update.* The newsletter is distributed NPPD-wide, and posted on the NPPD Office of Privacy intranet page.

## Office of the Chief Security Officer (OCSO)

- Provided a privacy training module in these OCSO classroom courses:
  - Security Orientation for Contractors
  - Security Orientation for Federal Employees
  - Safeguarding NSI: Your Responsibilities
  - Risk Management for Security Professionals
  - Operations Security
  - Sensitive But Unclassified Information
  - Acquisition Security Course
  - DHS Security Specialist Course. A DHS Privacy Office representative teaches the privacy module for this course.

## Office of the Inspector General (OIG)

- Initiated new privacy awareness training for onboarding employees by adding a 20-minute privacy training video produced by the DHS Privacy Office to the orientation program.
- Attended Privacy Compliance Boot Camp sponsored by the DHS Privacy Office to obtain in depth knowledge of privacy, and to better equip the OIG to address privacy issues.

## Transportation Security Administration (TSA)

- TSA Privacy engaged in privacy outreach with a number of advocacy groups, including ACLU, EPIC, CDT, CATO Institute, Liberty Coalition, Privacy Coalition, and Competitive Enterprise Institute, as well as within the federal privacy community.

## United States Citizenship and Immigration Services (USCIS)

- Continued to ensure that USCIS leadership, program managers, and system owners are aware of their responsibilities for protecting PII within the context of their position duties through the development and implementation of specialized training for these individuals. Topics of specialized training conducted: information sharing/disclosure, privacy incidents, social media training, and privacy compliance.
- Provided instructor-led training on "Privacy Incident Response" for record managers and other records personnel to ensure compliance with USCIS' and DHS' requirements to report privacy incidents, specifically when handling official records that contain PII and Sensitive PII. This training provides an overview of the requirements for reporting, investigating, and mitigating incidents.
- Provided Public Key Infrastructure and encryption training to leadership of the California Service Center.
- Created an Encryption Tip Bulletin to provide guidance to staff on when and how to encrypt emails containing sensitive information, specifically full Social Security numbers.
- Drafted onboarding documents to provide guidance to new employees on the USCIS Office of Privacy and how to safeguard PII and Sensitive PII.
- Provided privacy training to the Forms Management Branch, describing the privacy requirements for the forms review process, and the role of the USCIS Privacy Office in the forms review process.
- Published the USCIS Office of Privacy quarterly newsletters, entitled "Privacy Chronicles," to promote privacy awareness across USCIS and convey the importance of working together as partners to ensure that privacy is incorporated into all USCIS policies, guidance, and procedures.

- Implemented the Visual Tips Campaign, using digital signage to display tips on how to safeguard Sensitive PII. A new tip is displayed each quarter on all monitors at USCIS HQ facilities.
- Provided high level briefings to program offices on USCIS privacy policies, privacy compliance, how to safeguard PII, requirements for Computer Readable Extracts, and other privacy-related matters.
- Organized activities to observe Data Privacy Day 2017, to include live-streaming speakers, sharing privacy awareness materials, and conducting in-person training events.

## U. S. Coast Guard (USCG)

- Trained the USCG Office of Standard Evaluation and Development on the interface between privacy and information collections, and updates to the Department's privacy compliance documentation requirements based on new OMB guidance.

## U. S. Customs and Border Protection (CBP)

- Established multiple internal CBP Privacy Office working groups to ensure that privacy is embedded within CBP. These groups included a Communications Team, a Training Team, a Privacy Liaisons Team, an Information Governance Team, and a Mobile Applications Team.
- Trained new CBP Privacy Office staff through an internal eight-week Boot Camp.

## U.S. Immigration and Customs Enforcement (ICE)

- Conducted 13 New-Hire Orientation privacy trainings for a total of 157 ICE employees.
- Provided 10 New-Hire Orientation privacy trainings to ICE's Student and Exchange Visitor Program (SEVP), for a total of 64 SEVP employees.
- Provided one ICE Homeland Security Investigations, Office of Intelligence privacy training on October 24, 2016, discussing disclosures under the Privacy Act, the proper handling of Sensitive PII, and privacy incidents.
- Provided two Privacy/Information Assurance and Security Trainings for Information Technology Program Managers on November 9, 2016, for 27 employees, and November 14, 2016 for 39 employees, discussing Privacy and Information Security requirements that are built into the system development lifecycle.

## United States Secret Service (USSS)

- Trained new Special Agents and Uniformed Division Officer recruits in privacy rules of behavior, including limitations on sharing PII.
- Disseminated privacy awareness posters to Headquarters and Field Offices, and electronically via kiosks.
- Continued to conduct meetings of the PII Working Group to assess the use, collection, maintenance, and dissemination of PII within the Secret Service, and to identify additional privacy training needs to improve the handling and safeguarding of PII.
- Trained new hires on privacy protection best practices at bi-weekly new employee orientation classes.

# 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 Privacy Office or DHS Components or programs. The categories of complaints reflected in the following table are aligned with the categories detailed in the Office of Management and Budget's Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 14, 2008)*. U.S. citizens, Lawful Permanent Residents, visitors, and aliens submit complaints.[15]

**Table II: Type and Disposition of Complaints Received in the Reporting Period**

| Type of Complaint | Number of complaints received during the reporting period | Disposition of Complaint | | |
|---|---|---|---|---|
| | | Closed, Responsive Action Taken[16] | In Progress (Current Period) | In Progress (Prior Periods) |
| **Process & Procedure** | 0 | 1 | 0 | 1 |
| **Redress** | 148 | 147 | 1 | 0 |
| **Operational** | 604 | 605 | 4 | 0 |
| **Referred** | 1 | 1 | 0 | 0 |
| ***Total*** | ***753*** | ***754*** | ***5*** | ***1*** |

.

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.[17]

[15] *See* DHS Privacy Policy Guidance Memorandum 2007-01/Privacy Policy Directive 262-12, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons* (Jan. 7, 2009), available here: http://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2007-01-regarding-collection-use-retention-and. It should be noted that this policy was rescinded and replaced with new DHS policy on April 27, 2017. *See* DHS Privacy Policy Guidance Memoradum 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.

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

[17] 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.

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 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:

## U.S. Customs and Border Protection (CBP)

**COMPLAINT:** A complaint was received from a relative of a traveler. The traveler, who has a medical condition, was traveling with relatives when entering the U.S. The travelers were separated by CBP officers for questioning upon arrival at the Port of Entry, and the traveler with the medical condition was held for questioning. The relative attempted to explain that the medical condition caused the traveler to need assistance during questioning, but was told to leave the area or be arrested. The complainant asked if there is a form that can be placed on file for future trips so CBP is aware of the traveler's medical condition, as the experience was emotionally taxing and caused a setback in treatment.

**DISPOSITION:** The CBP Information Center processed the complaint and sent a response directly back to the complainant. The response apologized for the unpleasant experience, and suggested that the traveler have medical documentation explaining the condition, along with the contact information of a family member who can assist if needed for future arrivals at a CBP Port of Entry. The response also explained CBP's search authority, the secondary process, and mission to protect the Homeland. It also explained that it is not the intent of CBP to subject travelers to unwarranted scrutiny, but there are procedures in place to determine admissibility that unfortunately inconvenience law-abiding citizens at times in order to detect those that are involved in illicit activities. Finally, CBP offers any traveler the opportunity to speak with a supervisor to address any comments or concerns raised during the

inspection process, that all allegations of unprofessional conduct by any employee are taken seriously, and CBP appreciated the travelers initiative in bringing this matter to its attention.

## U.S. Immigration and Customs Enforcement (ICE)

**COMPLAINT:** ICE Privacy received a complaint from an ICE employee who alleged a supervisor improperly searched the employee's desk and released personal, private information about the employee.

**DISPOSITION:** On September 20, 2016, a report was issued by Homeland Security Investigations, *Investigative Programs – Investigative Findings – Management Inquiry* – concluding that the employee's claims were unsupported by its investigation. The matter was not referred to management.

# V. CONCLUSION

As required by the *Implementing Recommendations of the 9/11 Commission Act of 2007,* as amended, this semiannual report for FY17 summarizes the Privacy Office's activities from October 1, 2016 – March 31, 2017. The Privacy Office will continue to work with Congress, colleagues in other federal departments and agencies, and the public to ensure that privacy is protected in our homeland security efforts.