Department of Homeland Security

Privacy Office

Fiscal Year 2017 Semiannual Report to Congress

For the period April 1 – September 30, 2017

January 23, 2018

Homeland Security

FOREWORD

January 23, 2018

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's *Fiscal Year 2017 Semiannual Report to Congress,* covering the time period April 1 – September 30, 2017.[1]

Highlights

During the reporting period, the Privacy Office:

- Completed 854 Privacy Reviews, including 611 Privacy Threshold Analyses, 59 Privacy Impact Assessments, nine System of Records Notices, and one Privacy Compliance Review.
- Issued two new Privacy Policy Instructions, and updated one Privacy Policy Guidance Memorandum.

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* 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 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. 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 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 Trey Gowdy
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 Jerry Nadler
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 of 2002* 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, 2017***	
Type of Review	***Number of Reviews***
Privacy Threshold Analyses	611
Privacy Impact Assessments	59
System of Records Notices and associated Privacy Act Exemptions	9
Privacy Act (e)(3) Statements	2
Computer Matching Agreements	1
Data Mining Reports	0
Privacy Compliance Reviews	1
Privacy Reviews of IT and Program Budget Requests	0
Information Technology Acquisition Reviews[12] (ITAR)	171
Other Privacy Reviews	0
Total Reviews	***854***

[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 September 30, 2017, 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 59 PIAs: 29 new and 30 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-062 Homeland Security Information Network Leveraging Military Training Portal *(June 19, 2017)*

DHS, in close collaboration with Department of Defense (DoD) partners, designed the Leveraging Military Training (LMT) Portal, built on the Homeland Security Information Network (HSIN) platform, to enable DHS to share information with DoD relating to law enforcement needs and activities. Many DHS initiatives, programs, and operations require collaboration and communication among affected officials and stakeholders. The establishment of the LMT Portal is one way DHS and DoD have effectuated such collaboration, allowing authorized users to obtain, post, and exchange information, access common resources, and perform general communication and coordination with homeland security enterprise partners. DHS conducted this PIA to document and provide transparency about the LMT process, and to highlight the information that will be collected within the LMT Portal to facilitate collaboration between DHS and DoD and to provide accountability to Congress and the public.

DHS/CBP/PIA-044 Joint Integrity Case Management System *(July 18, 2017)*

U.S. Customs and Border Protection (CBP) created the Joint Integrity Case Management System (JICMS) to record claims of employee misconduct, manage criminal and administrative investigations, and to track employee and contractor disciplinary actions. The CBP Office of Professional Responsibility (OPR) and U.S. Immigration and Customs Enforcement (ICE) OPR are responsible for the overall operation of JICMS, however other DHS Components may use JICMS for their internal affairs case management. CBP conducted this PIA to assess the privacy risks and mitigations associated with JICMS because it collects, stores, and uses personally identifiable information (PII) about DHS employees, contractors, and members of the public.

DHS/FEMA/PIA-043 Contact Center Capability Modernization Program *(April 11, 2017)*

C3MP is a contact center management system designed to provide high quality support services to disaster survivors requesting assistance under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) during presidentially-declared disasters. It also provides the Federal

Emergency Management Agency (FEMA) the capability to evaluate employee and contractor performance when responding to applicants' calls in order to provide improved customer service. FEMA conducted this PIA because C3MP captures PII about applicants to provide status updates regarding their disaster applications. C3MP also gathers data about FEMA employees and contractors to monitor and enhance the quality of service provided by FEMA.

DHS/USSS/PIA-020 United States Secret Service Counter Surveillance Division Unmanned Aircraft Systems Program Test *(August 2, 2017)*
United States Secret Service's (USSS or Secret Service) Counter Surveillance Division (CSD) conducted a Proof of Concept to test and evaluate a tethered small Unmanned Aircraft System (sUAS) during a presidential visit to the Trump National Golf Club in Bedminster, New Jersey, in August 2017. The Proof of Concept helped determine the potential future use of tethered sUAS in supporting the agency's protective mission. The tethered sUAS used in the Proof of Concept operated using a microfilament tether that provided power to the aircraft and the secure video from the aircraft to the Operator Control Unit (OCU). The sUAS is equipped with electro-optical (EO) and infrared (IR) camera. USSS conducted this PIA to evaluate the privacy risks associated with tethered sUAS's surveillance and image capturing capabilities. This PIA was limited to covering the use of EO/IR sensors on a single tethered sUAS during one event. Any other use of these types of sensors by USSS on USSS aircraft—including sUAS—will be addressed in a future PIA.

Updated Privacy Impact Assessments

DHS/ALL/PIA-048(b) Foreign Access Management System *(April 10, 2017)*
The Foreign Access Management (FAM) program screens foreign nationals and foreign entities that seek physical and electronic access to DHS personnel, information, facilities, programs, or systems. DHS also provides this service to the United States Department of Agriculture (USDA) on a full-time basis, and occasionally to other agencies as needed. DHS has provided legacy support to USDA as a result of its presence at the DHS Plum Island Animal Disease Center (PIADC). This PIA update reflects the incorporation of non-DHS foreign access screening request data into the Integrated Security Management System (ISMS) Foreign Access Management System (FAMS). In addition, this update reflects the expanded support to USDA and other U.S. Government agencies to assess the feasibility and benefit of screening as a service for foreign nationals accessing non-DHS government personnel, information, facilities, programs, and systems. Unless otherwise noted, the information provided in previously published PIAs remains in effect.

DHS/CBP/PIA-024(b) Arrival and Departure Information System *(April 28, 2017)*
CBP's Arrival and Departure Information System (ADIS) contains biographic information, biometric indicators, and encounter data consolidated from various systems from DHS and the Department of State (DOS). ADIS facilitates the identification and investigation of individuals who may have violated their admission status by remaining in the United States beyond their authorized terms of entry. Other uses of ADIS include assisting in visa or immigration benefits eligibility determinations, providing information in support of national security, law enforcement, immigration and border management, intelligence purposes, as well as conducting background investigations on foreign nationals entering Federal Government facilities. This PIA was built upon existing documentation to provide a consolidated overview of the system and its functions, and discussed new data sharing arrangements with partner agencies.

DHS/CBP/PIA-030(c) Traveler Verification Service (TVS): Partner Process *(June 12, 2017)*
CBP continues to develop and expand its biometric entry-exit system for international flights at airports throughout the United States. CBP partners with commercial air carriers and airport authorities that will capture facial images of travelers as part of their business processes, and then send those photographs to CBP for use in the Traveler Verification Service (TVS). CBP matches the images against previously-captured photographs by using a cloud environment. CBP updated this PIA to provide the public with notice regarding CBP's plans to use PII collected by airlines and airport authorities, and CBP's use of facial matching technology in a cloud environment.

DHS/CBP/PIA-030(d) Traveler Verification Service (TVS): CBP-TSA Technical Demonstration *(September 25, 2017)*
In partnership with the Transportation Security Administration (TSA), CBP's latest biometric technical demonstration used the TVS cloud-based matching service to compare international travelers' photos captured by CBP against previously-captured photos. CBP updated this PIA to provide the public with notice regarding CBP's plans to use PII collected by CBP devices located at TSA security checkpoints.

DHS/USCIS/PIA-027(c) Asylum Division *(June 21, 2017)*
The Asylum Division of U.S. Citizenship and Immigration Services (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 maintains the Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System (APSS). Both systems, originally developed by the former Immigration and Naturalization Service (INS), are used by the USCIS Asylum Division to capture information pertaining to asylum applications, credible fear and reasonable fear screening processes, and applications for benefits provided by Section 203 of the Nicaraguan Adjustment and Central American Relief Act (NACARA §203). USCIS updated this PIA because the Asylum Division manages records and systems containing PII 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*.[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 September 30, 2017, 100 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the Privacy Office published six SORNs: two new and four updated. DHS also published four Privacy Act rulemakings: three Notices of Proposed Rulemakings and one Final Rule.

All DHS SORNs, Privacy Act 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/ALL-039 Foreign Access Management

This system of records allows DHS to collect and maintain records on foreign nationals who request physical or information technology system access to DHS and other U.S. Government partner agencies for which DHS provides screening support. Additionally, DHS issued a Notice of Proposed Rulemaking to exempt this system of records from certain provisions of the Privacy Act. *(82 FR 34971, July 27, 2017)*

- *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. *(82 FR 34884, July 27, 2017)*

DHS/ICE-016 FALCON Search and Analysis

FALCON Search and Analysis is a consolidated information management system that enables U.S. Immigration and Customs Enforcement (ICE) law enforcement and homeland security personnel to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal, civil, and administrative laws. *(82 FR 20905, May 4, 2017)*

- *Notice of Proposed Rulemaking*: In this proposed rulemaking, the Department proposed 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. *(82 FR 20844, May 4, 2017)*

[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.

Updated System of Records Notices

DHS/ALL-025 Law Enforcement Authority in Support of the Protection of Property Owned, Occupied, or Secured by the Department of Homeland Security

This system of records allows DHS to collect and maintain records on the results of law enforcement activities in support of the protection of property owned, occupied, or secured by DHS and its Components, including the Federal Protective Service, and individuals maintaining a presence or access to such property. DHS updated this system of records notice to, among other things, (1) modify the category of individuals, (2) modify the category of records, (3) modify two existing routine uses, and (4) add a new routine use. DHS also issued a Notice of Proposed Rulemaking to add a new exemption from certain provisions of the Privacy Act. This new exemption was needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. *(82 FR 27274, June 14, 2017)*

- *Notice of Proposed Rulemaking:* In this proposed rulemaking, the Department proposed to exempt portions of the system of records from additional provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. (*82 FR 27218, June 14, 2017*)

DHS/FEMA-002 Quality Assurance Recording System

This system of records allows FEMA to collect and maintain records on the customer service performance of its employees and contractors who interact with individuals who apply for the agency's individual assistance and public assistance programs. *(82 FR 32564, July 17, 2017)*

DHS/USCG-029 Notice of Arrival and Departure

This system of records allows the United States Coast Guard (USCG) to facilitate the effective and efficient entry and departure of vessels into and from the United States, and assist with assigning priorities for complying with maritime safety and security regulations. As part of the Department's ongoing effort to promote transparency regarding its collection of information, USCG updated its November 2015 system of records notice to explain its changes to the routine uses. Additional updates to this notice were explained in the November 2015 update. Further, this notice included non-substantive changes to simplify the formatting and text of the previously published notice. The Coast Guard re-issued this systems of records notice in its entirety for clarity and transparency. *(82 FR 32715, July 17, 2017)*

- *Final Rule:* DHS issued a final rule to extend the exemptions from certain provisions of the Privacy Act to the updated and reissued system of records titled "Department of Homeland Security/United States Coast Guard-029 Notice of Arrival and Departure System of Records." *(82 FR 32613, July 17, 2017)*

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking

This system of records contains information regarding transactions involving an individual as he or she passes through the U.S. immigration process, some of which may also be covered by separate SORNs. DHS primarily maintains information relating to the adjudication of benefits, investigation of immigration violations, and enforcement actions in Alien Files (A-Files). *(82 FR 43556, September 18, 2017)*

Privacy Compliance Reviews

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

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

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

United States Secret Service (USSS), July 21, 2017

On October 7, 2016, the DHS Office of Inspector General (OIG) issued report OIG-17-01, "*USSS Faces Challenges Protecting Sensitive Case Management Systems and Data*" that recommended that the DHS Privacy Office "conduct a systemic review with recommendations for ensuring USSS compliance with DHS privacy requirements." The DHS Privacy Office launched a PCR based on the OIG recommendation, focusing on USSS privacy compliance on December 2, 2016.

This PCR found that USSS requires significant resources to have an effective privacy program that incorporates robust outreach, collaboration, and oversight. The PCR made 12 recommendations for USSS to improve its privacy posture. The USSS Privacy Office was tasked with providing a written report and supporting documentation on the implementation status of all recommendations by July 2018.

II. ADVICE AND RESPONSES

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

Privacy Policy

The DHS Privacy Office issued the following new or updated privacy policies and related instructions during the reporting period:

New Privacy Policies

- *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 CPO 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* requires all DHS Components to appoint a Privacy Officer to oversee privacy compliance, policy, and oversight activities in coordination with the CPO.

Updated Privacy Policies

- *DHS Privacy Policy Guidance Memorandum 2017-01*. In response to Section 14 of Executive Order 13768[14], *Enhancing Public Safety in the Interior of the United States*, the Privacy Office rescinded its previous 2007 privacy policy (Privacy Policy Guidance Memorandum 2007-01/Privacy Policy Directive 262-12) titled *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.* To replace that policy and to clarify employee responsibilities under the several statutes that address the collection, use, retention, and dissemination of personal information, DHS issued a new policy on April 25, 2017 titled, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information.* The new policy, consistent with the Privacy Act, explains that immigrants and non-immigrants,[15] who are not subject to other legal protections (for example, the Judicial Redress Act of 2015), may only obtain access to their records through the Freedom of Information Act, and may not be granted amendment of their records upon request. Further, the new policy requires that DHS and Component decisions regarding the collection, maintenance, use, disclosure, retention, and disposal of information being held by DHS conform to an analysis consistent with the Fair Information Practice Principles (Privacy Policy Guidance Memorandum 2008-01/Privacy Policy Directive 140-06).

[14] EO 13768, Section 14 provides that "[a]gencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."

[15] An "immigrant" is defined as any alien who is not a "non-immigrant." See 8 U.S.C. § 1101(a)(15). A non-immigrant is an alien seeking temporary entry into the United States for a specific purpose.

Information Sharing and Intelligence Activities

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

The Privacy Office supports all five core DHS missions, as well as the important cross-cutting goal to *mature and strengthen homeland security by integrating information sharing and preserving privacy, oversight, and transparency in the execution of all departmental activities.*

There are currently more than 200 information-sharing agreements governing how DHS shares information. Requests for new agreements or amendments to existing agreements continue at a rapid pace. In accordance with numerous DHS Management Directives and Policy Instructions, the Privacy Office evaluates sharing requests that involve PII to mitigate privacy risks, incorporates privacy protections consistent with the DHS Fair Information Practice Principles, and audits or otherwise measures the effectiveness of those protections over time.

III. Training and Outreach

Mandatory Online Training

133,617 DHS personnel completed the mandatory computer-assisted privacy awareness training course, *Privacy at DHS: Protecting Personal Information*. This course is required for all personnel when they join the Department, and annually thereafter.

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

Classroom Training

3,888 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 provides an overview of all DHS Component offices.
- ***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 come from 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, role-based 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.

- ***The International Association of Privacy Professionals Global Summit*** – On April 20, 2017, in Washington, DC, the Deputy CPO moderated a panel on *Privacy Compliance Reviews*, comprising the DHS Director of Privacy Oversight, and Christopher Pierson, a member of the DHS Data Privacy and Integrity Advisory Committee.
- ***Data Privacy and Integrity Advisory Committee Meeting*** – On September 19, 2017, in Washington, DC, the Privacy Office hosted a public meeting of the Data Privacy and Integrity Advisory Committee (DPIAC). Members were briefed on biometrics, facial recognition, and immigration data, and tasked with submitting a report on best practices for protecting immigration statistics.
- ***Federal Privacy Council's Monthly Training Series*** – On September 28, 2017, in Washington, DC, the Federal Privacy Council hosted a seminar entitled *Privacy versus Security*. Panelists included the Deputy CPO and the Deputy Chief Information Security Officer.

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)

- Trained the Security Cadre, which has partnered with the FEMA Privacy Branch to implement the Privacy Points of Contact (PPOC) for Disaster Operations program. The PPOC for Disaster Operations program expands the Privacy Branch footprint into disaster operations offices and sites by having a PPOC on-site at each location to provide "just in time" privacy training, disseminate privacy resource materials, and conduct privacy compliance site assessments. The goal is to continue to embed and improve privacy protection and oversight in FEMA disaster operations environments and minimize risks for privacy incidents. This program was implemented during the response efforts for Hurricanes Harvey, Irma, and Maria.
- 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.
- 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 Branch also disseminated these materials across the enterprise to enhance PII protection as well as privacy incident reporting and mitigation.
- Emailed all FEMA staff in the wake of responding to three major hurricanes, reminding staff on how to properly safeguard PII during disaster response efforts.

Office of Intelligence and Analysis (I&A)

- Launched an internal privacy awareness campaign that will span a total of 10 months. The campaign utilizes monthly emails, flyers, and electronic messages to generate privacy awareness, including: defining PII and Sensitive PII, PII safeguarding tips, and internal and external data sharing procedures.

National Protection and Programs Directorate (NPPD)

The NPPD Office of Privacy published two privacy related articles in NPPD's weekly newsletter, entitled *NPPD Vision*. The newsletter is distributed NPPD-wide. The articles covered subjects such as Telework Guidance and Email Best Practices. In addition, the Office of Privacy published two issues (June and September) of its quarterly newsletter, entitled the *NPPD Privacy Update.* The newsletter is distributed NPPD-wide and posted on the NPPD Office of Privacy internal intranet page.

NPPD Privacy Office staff conducted the following training events during the reporting period:

- April 25 2017: An NPPD Privacy Analyst provided the privacy brief during Information Technology Acquisition Review (ITAR) training at the Office of Cybersecurity & Communications (CS&C) to 20 Contracting Officer Representatives.
- April 25 and 27, 2017: An NPPD Privacy Analyst provided Component privacy training to 21 employees/contractors during FOIA training at the Federal Protective Service (FPS).
- April 27, 2017: NPPD Privacy Analysts participated in "Take Your Daughters and Sons to Work Day" at NPPD by providing a privacy presentation to approximately 160 children. This presentation was part of an annual event that introduces young girls and boys to a variety of occupations and allows them to expand their career horizons.
- April 27, 2017: NPPD Director, Privacy, provided *IT Security for Privacy Professionals* training for week six of the Federal Privacy Council's boot camp.
- June 14, 2017: An NPPD Privacy Analyst gave a privacy presentation during a quarterly Office of Infrastructure Protection (IP) Contracting Officer Representative (COR) training to 45 IP CORs.
- June 14, 2017: An NPPD Privacy Analyst provided Component privacy training to 30 employees/contractors during acquisition training at the Federal Protective Service (FPS).
- June 23, 2017: OBIM's Section Chief for Privacy, Policy, and FOIA, and the Sr. Privacy Analyst gave a presentation to Master's Degree students at the University of Texas at Austin's Center for Identity on how OBIM's large scale enterprise database system, IDENT/HART, handles identity information management and privacy protection.
- June 27, 2017 and August 15, 2017: NPPD Privacy analysts provided role-based training for the Office of Human Capital with a total of 58 attendees.
- September 13 and 27, 2017: NPPD Privacy analysts provided privacy awareness regarding the privacy requirements (drafting of a Forms PTA) through participation in an Information Compliance webinar to a total of 67 NPPD employees/contractors regarding the Paperwork Reduction Act (PRA) process.
- September 14, 2017: NPPD Office of Biometric Identity Management (OBIM) Section Chief for Privacy, Policy, and FOIA participated in a panel discussion on Screening and Biometric Interoperability at the Armed Forces Communications and Electronics Association (AFCEA)'s Federal Identity (FedID) Conference. Aspects of the panel discussion focused on the ways OBIM embeds privacy protections into its organization.
- September 14, 2017: NPPD Director, Privacy presented at the AFCEA FedID Conference on *Practical Applications of Privacy and Civil Liberties*, a session about the privacy requirements integrated throughout the latest revision of the National Institute of Standards and Technology (NIST) Special Publication 800-63-3, *Digital Identity Guidelines*. The new NIST guidance aims to help IT implementers and privacy programs better collaborate on developing secure digital identity solutions while managing privacy risk.
- September 27, 2017: NPPD Privacy Analysts provided role-based privacy training to 10 attendees from the NPPD Executive Secretariat (ExecSec).

- October 2, 2017: NPPD conducted role-based training for FPS Personnel Security Division for 38 individuals located in the NCR and regional offices.

Transportation Security Administration (TSA)

- TSA Privacy conducted eight different outreach activities, including meetings with privacy advocates, privacy compliance presentations to TSA Information System Security Owners (ISSO's) and public relations personnel, and a Sensitive PII safeguarding reminder within a National Shift Brief disseminated to over 400 airports.

United States Citizenship and Immigration Services (USCIS)

Training:

- Presented on information sharing with foreign partners for the Europe, Latin American and Asia regions of the Refugee, Asylum and International Operations directorate.
- Provided support on the Mandatory Training Advisory Committee for fiscal year 2017. USCIS Privacy provides guidance to the committee from a privacy viewpoint on mandatory trainings within USCIS.
- Conducted encryption training to the California Service Center Operations, and disseminated an encryption bulletin to all USCIS personnel on the agency's encryption policy.
- Provided Privacy Incident Response, instructor-led training for record managers and staff to ensure they understand the privacy incident reporting requirements. This training provides an overview of the requirements for reporting, investigating, and mitigating incidents.

Outreach:

- January 2017: Organized privacy activities to observe Data Privacy Day, to include live-streaming speakers, sharing privacy awareness materials, and conducting in-person training events.
- February 2017: Held the annual Privacy Contest to recognize the program efforts in implementing privacy protections during daily operations, and promoting a culture of privacy.
- May 9, 2017: Conducted a Knowledge café on privacy compliance for employees working within the Verification Division, covering the privacy compliance process, privacy laws and policies, and privacy artifacts (i.e., PTAs, PIAs, and SORNs).
- June 27, 2017: Hosted a brown bag session entitled, *Millennials in the Workforce & Privacy*.
- July 2017: Participated in the Los Angeles inter-governmental roundtable at the invitation of the Community Relations Officer from the Western Region. USCIS leadership and other DHS Components met to discuss emerging issues with partners from many of the area's local consulates, as well as universities with substantial exchange student populations, and local libraries who work to assist immigrants with preparation for the civics and language tests.
- August 21, 2017: Hosted a privacy awareness training event featuring Charles Cutshall from the Office of Management and Budget (OMB), who presented on the role of OMB and privacy policy oversight. After the presentation, Privacy Awareness Training was presented to 217 USCIS employees, and a privacy tips brochure was provided to participants.
- August 2017: Assisted with the formulation of a Leadership Handbook for new and incoming District Directors to highlight resources available to this level of leadership, and to reinforce standards of operation. A section on privacy was incorporated within handbook that includes: 1) when and how to contact a Regional Privacy Officer, 2) when and how to file a Significant Incident Report in the event of a suspected or confirmed breach/incident, 3) reminders related to the compliance process, and 4) tips on what constitutes PII/Sensitive PII.

- Promoted privacy practices and advertised the services of the USCIS privacy program at both the Western Region District Director's conference and the Field Office Director's conference.
- Provided high level briefings to program offices on USCIS privacy policies relating to 1) privacy compliance, 2) how to safeguard PII/SPII, 3) requirements for Computer Readable Extracts (CREs), and 4) other privacy related policies.
- Reviewed multiple Agile development processes to ensure privacy is considered throughout this fast-paced and often changing environment. In the Agile environment, checkpoints for privacy have been built into these processes to quickly identify privacy issues, with a path to remedy issues and halt production that may pose undue privacy problems.
- Disseminated Privacy Tips on promoting privacy awareness and guidance on how to protect PII/Sensitive PII from unauthorized use, handling, and disclosure.
- Disseminated a monthly Internal Privacy Bulletin to inform staff of recent and upcoming privacy activities.
- Published the *Privacy Chronicles* to alert USCIS personnel of any new privacy policies and upcoming events/activities, and to reinforce the importance of embedding privacy in all USCIS policies, guidance, and procedures.

U.S. Immigration and Customs Enforcement (ICE)

Training:

- 13 New-Hire Orientation privacy trainings for a total of 152 ICE employees.
- 13 ICE Student and Exchange Visitor Program New-Hire Orientation privacy trainings for 45 employees.
- Four ICE Office of Human Capital trainings for mission support staff on August 17, 2017, August 24, 2017, September 21, 2017, and September 28, 2017, for a total of 158 employees, addressing general privacy and records management concepts, and an overview of Freedom of Information Act (FOIA) requests and responses.
- One ICE Office of Public Affairs (OPA) training for public affairs staff on September 20, 2017 for a total of 60 employees, discussing public disclosures, and coordination between OPA and ICE IGP.
- One Counterterrorism and Criminal Exploitation Unit (CTCEU) privacy training on July 12, 2017 for 70 employees and contractors in the CTCEU analyst role, discussing the collection, use, and disclosure of information as a result of the new Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*.
- One ICE Office of Congressional Affairs privacy training on August 29, 2017, for approximately 10 employees, discussing media disclosure guidance for Appendix A releases as well as congressional requests for information.

Outreach:

- September 14, 2017: The ICE Assistant Director for Information Governance & Privacy spoke on the *Identity and Immigration* panel at the Federal Identity Forum and Exposition and Armed Forces Communications and Electronics Association Homeland Security Conference.

United States Secret Service (USSS)

- Hosted a Privacy Awareness Day event on June 28, 2017 to educate staff on privacy best practices and federal privacy laws.
- 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 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 OMB'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.[16]

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[17]	In Progress (Current Period)	In Progress (Prior Periods)
Process & Procedure	1	2		
Redress	210	210		
Operational	855	854	6	
Referred	0	0		
Total	***1,064***	***1,066***	***6***	***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.[18]

[16] *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 a new DHS policy on April 27, 2017. *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.

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

[18] 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 privacy complaints received during this reporting period, along with their disposition:

Federal Emergency Management Agency (FEMA)

COMPLAINT:
An employee from the Maryland National Processing Service Center, which is a FEMA survivor call center, reported that a call-down spreadsheet containing personal cell phone numbers was sent to his entire team. The individual complained because he did not want non-supervisory personnel to have his personal contact information. FEMA Privacy contacted the employee's supervisor and counselled them on the appropriate safeguarding of PII and call-down rosters. The supervisor agreed to send blank forms in the future requesting that employees provide their personal contact information only to the supervisor. FEMA Privacy also provided the supervisor with remedial privacy training.

COMPLAINT:
An employee complained that his supervisor intentionally disclosed his medical condition to other employees and contractors in his division. FEMA Privacy interviewed the supervisor and complainant, and upon learning additional details of the complaint, determined that a breach had not occurred. Nonetheless, FEMA Privacy counseled the employee's supervisor on the appropriate treatment of PII and Sensitive PII, which, in this case was health-related information, and sent formal notification letters to the complainant and the supervisor.

Transportation Security Administration

COMPLAINT:
A TSA employee complained to the TSA Privacy office that her privacy rights were violated when her supervisor requested her to provide documentation of her medical condition. TSA Privacy assured the employee that her supervisor's request for medical documentation was required by TSA Management Directives governing leave (providing citations to the applicable sections) and not an attempt to violate her privacy.

U.S. Customs and Border Protection (CBP)

COMPLAINT:
A traveler attending a scientific research conference requested clarification on CBP searches of electronic devices. The individual expressed concern that 6,000 attendees would be coming to the conference, many from foreign countries. Specifically the individual requested clarification of the policies governing border searches of mobile phones and computers. The CBP Information Center (CIC) processed the complaint and sent a response directly back to the complainant. In the response, the complainant was notified of the specific laws that support CBP's authority to review electronic devices. Also, CBPs policy regarding travelers repacking their own belongings after conducting the inspection so as to minimize accusations of missing objects was also clarified.

COMPLAINT:
A male traveler complained of discrimination based on national origin, after being sent to secondary inspection at the Nogales border crossing. The CBP Information Center processed the complaint and sent a response directly back to the complainant. The response gave the complainant information for how to seek redress from DHS. Additionally, the complaint was sent to the DHS Office for Civil Rights and Civil Liberties, and the CBP Office of Professional Responsibility for further review and possible investigation.

COMPLAINT:
A traveler arriving at the Port of Miami complained that his personal mobile phone was searched, and that his identifying numbers were recorded and his photographs reviewed. The complainant stated they felt their rights were violated as some of the photos were of him and his wife and not meant to be seen publicly. The complainant requested an explanation of why the search was allowed. CBP Information Center processed the complaint and sent a response directly back to the complainant. The response apologized for the unpleasant experience and 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 of its employees are taken seriously, and CBP appreciated the traveler's initiative in bringing this matter to its attention.

U.S. Immigration and Customs Enforcement (ICE)

COMPLAINT:
ICE received a complaint from an ICE employee questioning the scope of the data collection requested by the program office to identify interested employees for a planned training event held at the Federal Law Enforcement Training Center (FLETC). As part of the announcement, those interested in participating were asked to submit Sensitive PII, including DOB and SSN, to a group email box. The Privacy Division conducted an inquiry that identified several issues of concern regarding the collection and use of Sensitive PII. The Privacy Division noted that while the Sensitive PII was necessary during the course registration process, it was determined to be an over-collection during the training nomination phase. Additionally, there were noted issues about need to know for all of the recipients of the email distribution list, and processes for handling and storing the information. The Privacy Division requested that the program office correct these areas of concern to specifically reduce the amount of data collected when nominating employees for training, and the processes for collecting and transferring Sensitive PII as part of FLETC's registration process.

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 April 1 – September 30, 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.