

# PRIVACY

## Department of Homeland Security

Privacy Office

Fiscal Year 2015 Second Semiannual Report to Congress

*For the period April 1, 2015 – September 30, 2015*

*December 21, 2015*



Homeland  
Security

## Foreword

*December 21, 2015*

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's *Fiscal Year 2015 Semiannual Report to Congress*, covering the time period April 1 – September 30, 2015.<sup>1</sup>

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*<sup>2</sup> requires the Privacy Office to report on the following activities:

- Number and types of privacy reviews of Department actions undertaken;
- Type of advice provided and the response given to such advice; and
- Number and nature of privacy complaints received by DHS for alleged violations, along with a summary of the disposition of such complaints.



In addition, we include information on privacy training and awareness activities conducted by the Department to help prevent privacy incidents.

The Chief Privacy Officer is the first statutorily-mandated Chief Privacy Officer in the Federal Government. Section 222 of the *Homeland Security Act of 2002* (Homeland Security Act),<sup>3</sup> sets forth the responsibilities of the Privacy Office. The mission of the Privacy Office is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. Within DHS, the Chief Privacy Officer implements Section 222 of the Homeland Security Act, the *Privacy Act of 1974*,<sup>4</sup> the *Freedom of Information Act*,<sup>5</sup> and the *E-Government Act of 2002*,<sup>6</sup> along with numerous other laws, executive orders, court decisions, and DHS policies that impact the collection, use, and disclosure of Personally Identifiable Information (PII) by DHS.

---

<sup>1</sup> 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 will cover the following time periods: April – September and October – March.

<sup>2</sup> 42 U.S.C. § 2000ee-1(f).

<sup>3</sup> 6 U.S.C. § 142.

<sup>4</sup> 5 U.S.C. § 552a.

<sup>5</sup> 5 U.S.C. § 552.

<sup>6</sup> 44 U.S.C. § 3501 note.

Please direct any inquiries about this report to the Privacy Office at 202-343-1717 or [privacy@dhs.gov](mailto:privacy@dhs.gov). More information about the Privacy Office, along with copies of prior reports, is available on the Web at: [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

Sincerely,

A handwritten signature in black ink, appearing to be 'K. Neuman', with a long horizontal line extending to the right.

Karen L. Neuman  
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 Ron Johnson**

Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

**The Honorable Tom Carper**

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 Patrick Leahy**

Ranking Member, U.S. Senate Committee on the Judiciary

**The Honorable Richard Burr**

Chairman, U.S. Senate Select Committee on Intelligence

**The Honorable Dianne Feinstein**

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 2015  
SECOND SEMIANNUAL  
SECTION 803 REPORT TO CONGRESS**

**Table of Contents**

I.	FOREWORD .....	1
II.	LEGISLATIVE LANGUAGE .....	5
III.	PRIVACY REVIEWS .....	6
	A. Privacy Impact Assessments .....	8
	B. System of Records Notices .....	10
	C. Privacy Compliance Reviews .....	11
IV.	ADVICE AND RESPONSES.....	13
	A. Privacy Training and Awareness .....	13
	B. Privacy Office Awareness & Outreach .....	15
	C. Component Privacy Office Awareness & Outreach .....	17
V.	PRIVACY COMPLAINTS AND DISPOSITIONS.....	21
VI.	CONCLUSION.....	24

## II. LEGISLATIVE LANGUAGE

Section 803 of the *9/11 Commission Act of 2007*,<sup>7</sup> 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.”

---

<sup>7</sup> 42 U.S.C. § 2000ee-1.

### III. PRIVACY REVIEWS

The Privacy Office reviews programs and information technology (IT) systems that may have a privacy impact. For purposes of this report, 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*,<sup>8</sup> the *Homeland Security Act of 2002*,<sup>9</sup> and DHS policy;
3. System of Records Notices, as required under the Privacy Act, and any associated Final Rules for Privacy Act exemptions;<sup>10</sup>
4. Privacy Act Statements, as required under the Privacy Act,<sup>11</sup> to provide notice to individuals at the point of collection;
5. Computer Matching Agreements, as required under the Privacy Act;<sup>12</sup>
6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*;<sup>13</sup>
7. Privacy Compliance Reviews, per the authority granted to the Chief Privacy Officer by the *Homeland Security Act of 2002*;<sup>14</sup>
8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) Exhibit 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board; and
9. Other privacy reviews, such as implementation reviews for information sharing agreements.

---

<sup>8</sup> 44 U.S.C. § 3501 note. 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](http://www.whitehouse.gov/omb/memoranda_m03-22).

<sup>9</sup> 6 U.S.C. § 142.

<sup>10</sup> 5 U.S.C. § 552a(j), (k). 5 U.S.C. § 552a(e)(4). *See also* OMB Circular No. A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6428 (Feb. 20, 1996), *as amended*, 65 Fed. Reg. 77,677 (Dec. 12, 2000), *available at*: [https://www.whitehouse.gov/omb/circulars\\_a130](https://www.whitehouse.gov/omb/circulars_a130).

<sup>11</sup> 5 U.S.C. § 552a(e)(3).

<sup>12</sup> 5 U.S.C. § 552a(o)-(u).

<sup>13</sup> 42 U.S.C. § 2000ee-3.

<sup>14</sup> 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.

<b>Table I</b>	
<b>Reviews Completed: <i>April 1 - September 30, 2015</i></b>	
<b>Type of Review</b>	<b>Number of Reviews</b>
Privacy Threshold Analyses	337
Privacy Impact Assessments	28
System of Records Notices and associated Privacy Act Exemptions	12
Privacy Act (e)(3) Statements	3
Computer Matching Agreements	1
Data Mining Reports	0
Privacy Compliance Reviews	4
Privacy Reviews of IT and Program Budget Requests <sup>15</sup>	108
Other Privacy Reviews	0
<b><i>Total Reviews</i></b>	<b>493</b>

<sup>15</sup> The Chief Information Office prepares a privacy score once a year as part of its Office of Management and Budget Exhibit 300 reporting. Reviews for this category are calculated only during this semi-annual reporting period.

## A. 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 systems not currently subject to a PIA, the Department conducts a triennial review of existing PIAs to assess and confirm that the systems still operate within the originally published parameters. After the Department completes a triennial review, it updates any previously published PIAs to inform the public that it has completed a review of the affected systems.

During the reporting period, the Office published 28 PIAs. All published DHS PIAs are available on the Privacy Office website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy); we include a summary of key PIAs here, along with a hyperlink to the full text.

### [DHS/CBP/PIA-003\(b\) Automated Commercial Environment](#) (July 31, 2015)

The Automated Commercial Environment (ACE) is the backbone of U.S. Customs and Border Protection's (CBP) trade information processing and risk management activities system and is the key to implementing many of the agency's trade transformation initiatives. ACE allows efficient facilitation of imports and exports and serves as the primary system used by U.S. Government agencies to process cargo. ACE serves as the "Single Window" for trade facilitation as mandated by Executive Order 13659, *Streamlining the Export/Import Process for America's Businesses*. CBP published this PIA for ACE because ACE collects, maintains, uses, and disseminates import and export information from the trade community that contains PII.

### [DHS/S&T/PIA-029 Data Collection for the Centralized Hostile Intent Project](#) (June 9, 2015)

The Centralized Hostile Intent (CHI) program within DHS' Science and Technology Directorate (S&T) collects video images of trained actors posing as passengers, as well as members of the traveling public at the Theodore Francis Green Memorial State Airport in Providence, Rhode Island. The program goals of CHI are to assess whether behavioral indicators of malicious intent can be observed by trained professionals (e.g., Transportation Security Administration (TSA) Behavior Detection Officers) from video images in a remote environment. Remote screening offers the potential for the TSA to expand the scale of its behavior detection program without correspondingly increasing staffing costs. PII is collected in the form of video images containing the faces and bodies of trained actors and members of the traveling public. This PIA addresses privacy issues associated with the collection of the video data for the CHI program and updates the previously published PIA for "Project Hostile Intent Technology."

### [DHS/ALL/PIA-050 DHS Trusted Identity Exchange \(TIE\)](#) (April 2, 2015)

The Trusted Identity Exchange (TIE) system is a privacy-enhancing DHS Enterprise Service that enables and manages the digital flow of identity, credential, and access-management data for DHS employees and contractors. It does so by establishing connections to various internal authoritative data sources, and provides a secure, digital interface to other internal DHS consuming applications. A consuming application is any DHS system that requires some form of identity, credential, and access-management data in order to grant logical or physical access to a DHS protected resource. DHS published this PIA because TIE accesses and disseminates PII.

[DHS/ALL/PIA-051 DHS Data Framework – Interim Process to Address an Emergent Threat](#) (*April 15, 2015*)

This PIA explains DHS' plan to expedite its ability to meet a critical mission need through the use of an interim manual data transfer process. Specifically, DHS has a critical mission need to perform classified queries on its unclassified data in order to identify individuals supporting the terrorist activities of: (1) the Islamic State of Iraq and the Levant (ISIL), (2) al-Qa'ida in the Arabian Peninsula (AQAP), (3) al-Nusrah Front, (4) affiliated offshoots of these groups, or (5) individuals seeking to join the Syria-Iraq conflict. (These individuals are often referred to as "foreign fighters" by the media and in public discourse.) The ability to perform classified searches of unclassified data for this uniquely time sensitive purpose allows DHS to better identify and track foreign fighters who may seek to travel from, to, or through the United States. This type of comparison is a long-standing mission need; however, the specific threat has shortened the timeframe in which DHS must meet the need.

[DHS/CBP/PIA-026 Biometric Exit Mobile Air Test](#) (*June 18, 2015*)

CBP is conducting a Biometric Exit Mobile Air Test for certain aliens departing the United States on selected international flights at selected U.S. airports. The Biometric Exit Mobile Air Test is designed to test a new biometric exit concept of operations at selected airports. During the test, CBP officers use a wireless handheld device at the departure gate to collect biometric and biographic data and to test outbound enforcement policies and workforce distribution procedures. The Department is also transferring the privacy compliance documentation for biometric air exit programs to the CBP privacy impact assessment inventory because CBP is the operational Component within the Department that is responsible for biometric and biographic entry and exit operations.

## B. System of Records Notices

System of Records Notices (SORN) receive biennial reviews 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.

During the reporting period, the Privacy Office published 10 SORNs. A sampling of these documents are summarized below, with a hyperlink to the *Federal Register Notice*. All DHS SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act Exemptions are available on DHS' Privacy Office's website, located at [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

### [DHS/CBP-007 Border Crossing Information \(BCI\)](#) (May 11, 2015)

This system of records authorizes CBP to collect and maintain records on border crossing information for all individuals who enter, are admitted or paroled into, and (when available) exit from the United States, regardless of method or conveyance. Border crossing information includes certain biographic and biometric information, photographs, certain mandatory or voluntary itinerary information provided by air, sea, bus, and rail carriers, or any other forms of passenger transportation, and the time and location of the border crossing.

### [DHS/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records](#) (May 27, 2015)

This system of records authorizes the Office of Operations Coordination, National Operations Center (NOC) to fulfill its statutory mandate pursuant to 6 U.S.C. § 321d(b) to provide situational awareness and establish a common operating picture, through monitoring activities on social media for information, for the entire Federal Government, and for state, local, and tribal governments, as appropriate, to ensure that critical terrorism and disaster-related information reaches government decision-makers.

### [DHS/CBP-001 Import Information System](#) (August 17, 2015)

This system of records authorizes CBP to collect and maintain records on all commercial goods imported into the United States, along with carrier, broker, importer, and other Automated Commercial Environment-International Trade Data System Portal user account and manifest information. The purpose of this system of records is to track, control, and process all commercial goods imported into the United States. This facilitates the flow of legitimate shipments, and assists CBP in securing U.S. borders and targeting illicit goods.

### [DHS/CBP-020 Export Information System](#) (September 2, 2015)

The Export Information System (EIS) is the central point through which CBP collects and maintains export data and related records to facilitate DHS's law enforcement and border security missions. DHS uses EIS to ensure the safety and security of cargo, prevent smuggling, and enforce export and other applicable U.S. laws.

## C. Privacy Compliance Reviews

The Privacy Office uses Privacy Compliance Reviews (PCR) to ensure DHS programs and technologies implement and maintain appropriate privacy protections for PII. Consistent with the Office's unique position as both an advisor and oversight body for the Department's privacy-sensitive programs and systems, the PCR is a collaborative effort that helps improve a program's ability to comply with existing privacy compliance documentation, including PIAs, SORNs, and formal agreements such as Memoranda of Understanding and Memoranda of Agreement. PCRs may result in public reports or internal recommendations, depending upon the sensitivity of the program under review.

Public PCR reports are available on the Privacy Office website, [www.dhs.gov/privacy](http://www.dhs.gov/privacy), under "Investigations and Compliance Reviews."

During the reporting period, the Privacy Office completed four PCRs:

1. [Enhanced Cybersecurity Services \(ECS\)](#) (*April 10, 2015*)  
ECS is a voluntary DHS program in which NPPD's Office of Cybersecurity and Communications provides indicators of malicious cyber activity to participating commercial service providers. The purpose of the program is to assist the owners and operators of critical infrastructure in enhancing their ability to protect their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program. In performing the PCR, the Privacy Office made four recommendations but nonetheless found that NPPD developed the ECS Program and its related processes with privacy-protective objectives in mind. NPPD continues to operate the ECS Program and its related processes with strong privacy oversight, which allows NPPD to identify and mitigate privacy risks as the program evolves and matures.
2. [Media Monitoring and Situational Awareness Initiative](#) (*May 21, 2015*)  
PCRs are a key aspect of the layered privacy protections built into the Media Monitoring Initiative to ensure that the protections described in the May 2015 PIA Update and the May 2015 SORN are followed. In performing the PCR, the Privacy Office found that the Office of Operations Coordination, National Operations Center, continues to be in compliance with the privacy requirements identified in these documents, and made three recommendations to continue to improve its ability to demonstrate compliance with privacy requirements.
3. [Passenger Name Records](#) (*June 26, 2015*)  
The Privacy Office reviewed policies, practices, and departmental activities of the Department's collection and use of Passenger Name Records (PNR) from June 1, 2013 to February 1, 2015, including the details of PNR received and reviewed by DHS and information sharing practices with non-DHS entities. During the course of this PCR, the Privacy Office found PNR policies and practices, including how PNR is received, used, and disseminated by CBP, to be substantially compliant with related provisions in the Automated Targeting System PIA and SORN. Nonetheless, the Privacy Office made 12 recommendations to continue to improve its ability to demonstrate compliance with privacy requirements.

The review also found DHS to be in compliance with the terms of the 2011 Agreement between the United States and the European Union on the use and transfer of PNR to the Department by air carriers operating flights between the United States and the European Union (2011 Agreement). The PCR informed the discussions during the joint review of the 2011 Agreement with the European Commission on July 1-2, 2015, which was hosted by DHS' Chief Privacy Officer. During the joint review, DHS thoroughly explained DHS's use and protection of PNR, and presented its compliance with the terms of the 2011 Agreement. The European Commission is expected to publish the results of its review by the end of 2015.

4. [Office of the Chief Human Capital Officer](#) *(September 30, 2015)*

In response to privacy incidents at the Office of the Chief Human Capital Officer (OCHCO), the Privacy Office submitted an action memo on March 27, 2014 to the DHS Chief Human Capital Officer with 12 recommendations to strengthen the culture of privacy within the office. In April 2015, the Privacy Office initiated a PCR of OCHCO's implementation of the 12 recommendations and compliance with DHS privacy policy. In performing the PCR, the Privacy Office found that some concerns raised in the 2014 Memo remain, and several recommendations from the 2014 Memo have yet to be fully implemented. As a result, the Privacy Office made an additional 25 recommendations to effectuate a culture of privacy within OCHCO.

## IV. ADVICE AND RESPONSES

### A. Privacy Training and Awareness

During the reporting period, DHS conducted the following privacy training:

#### *Mandatory Online Training*

89,218 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.

12,228 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 any Privacy Office-adjudicated Component Social Media Operational Use Template(s).

#### *Classroom Training*

5,685 DHS personnel attended instructor-led privacy training courses, including the following:

- **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<sup>16</sup> also offer privacy training for new employees when they onboard. 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.
- **Compliance Boot Camp**: The Privacy Office trained the Component Privacy Points of Contact in compliance best practices, including how to draft PTAs, PIAs and SORNs.
- **FOIA Training**: This periodic training is tailored to staff responsible for gathering records in response to FOIA requests, and for FOIA staff processing records.
- **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 Information Security Specialist Course**: The Privacy Office provides privacy training each month to participants of this week-long training program.

---

<sup>16</sup> Ten DHS offices and components have a Privacy Officer. These designated privacy officers can be found here: <http://www.dhs.gov/privacy-office-contacts>.

- 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 Training for Fusion Centers: The Privacy Office collaborates with the Office for Civil Rights and Civil Liberties to provide periodic privacy training for privacy officers at state and local fusion centers.
- Privacy Briefings for Headquarters Staff: During this reporting period, the Privacy Office continued a year-long privacy awareness campaign throughout the DHS Headquarters division to provide customized classroom privacy awareness briefings to employees and contractors. The goal is to increase awareness of DHS privacy policy and the importance of incorporating privacy protections into any new program or system that will collect PII.

## B. Privacy Office Awareness & Outreach

### *Publications*

Privacy and Civil Liberties Assessment Report: Pursuant to [Executive Order 13636](#)<sup>17</sup> (EO 13636), *Improving Critical Infrastructure Cybersecurity* (February 12, 2013), senior agency officials for privacy and civil liberties are required to assess the privacy and civil liberties impacts of the activities their respective departments and agencies have undertaken to implement EO 13636, and to publish their assessments annually in a report compiled by the Privacy Office and the Office for Civil Rights and Civil Liberties. This year's [report](#) was published on April 10, 2015<sup>18</sup>.

### *Congressional Testimony*

The Chief Privacy Officer testified before the House Committee on Oversight and Government Reform on June 3, 2015 at a hearing, "Ensuring Agency Compliance with the FOIA," along with chief Freedom of Information Act (FOIA) officers from two other agencies. The hearing examined the processes agencies use to meet FOIA's legal requirements, and explored barriers to effective and efficient compliance from the FOIA officer's perspective.

### *Meetings & Events*

- [RSA Conference](#) – On April 20-24, 2015, the Chief Privacy Officer attended this conference in San Francisco, California.
- [American Bar Association Spring Meeting](#) – On April 30, 2015, the Chief Privacy Officer participated in a roundtable discussion on the "Rise of the Chief Privacy and Data Protection Officer" in Washington, DC.
- [FedScoop's Federal Executive Roundtable](#) – On May 12, 2015, the Deputy Chief Privacy Officer discussed the DHS Data Framework in Washington, DC.
- [Centre for Information Policy Leadership Annual Executive Retreat](#) – On May 19, 2015, the Chief Privacy Officer attended this event in Washington, DC.
- [Privacy Advocate Meeting](#) – In June 2015, privacy advocates met with representatives from the Office of the General Counsel and the National Protection and Programs Directorate, who presented an overview of the Automated Indicator Sharing Initiative.
- [Privacy Matters Symposium](#) – On June 9, 2015, the Deputy Chief Privacy Officer attended this event hosted by the Veteran's Administration in Washington, DC.

---

<sup>17</sup> <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

<sup>18</sup> <http://www.dhs.gov/publication/2015-executive-order-13636-privacy-and-civil-liberties-assessment-report>.

- Summer Technology Exchange – On June 17, 2015, the Privacy Office’s Senior Director for Policy and Oversight gave a presentation on Executive Order 13636 at this workshop sponsored by the Department of Health and Human Services in Bethesda, Maryland.
- Joint Review of the 2011 Passenger Name Records (PNR) Agreement – On July 1-2, 2015, the Chief Privacy Officer hosted a joint review of the 2011 PNR Agreement with the European Commission where DHS thoroughly explained DHS’s use and protection of PNR and presented its compliance with the terms of the 2011 Agreement. The European Commission is expected to publish the results of its review by the end of 2015.
- Data Privacy and Integrity Advisory Committee Meeting – On September 10, 2015, the Privacy Office held a public meeting of the Data Privacy and Integrity Advisory Committee, both online and in-person in Washington, DC. Members were briefed on the draft Privacy Office mobile application policy, as well as on privacy incidents at DHS. Committee members received a tasking from the Chief Privacy Officer on privacy incidents.
- Privacy Law Salon – On September 11, 2015, the Chief Privacy Officer participated in a roundtable discussion on privacy policy making hosted by The George Washington University Law School in Washington, DC.

## C. Component Privacy Office Awareness & Outreach

### *Federal Emergency Management Agency (FEMA)*

- Supported the Workplace Transformation initiative by conducting privacy training and site risk analysis in the National Capital Region to reinforce best practices for securing PII during office relocations as well as in an open work environment.
- Disseminated privacy fact sheets, posters, and other best practice materials to increase privacy awareness and promote the protection of PII as well as the reporting of privacy incidents.
- Provided specialized privacy training to information professionals and remedial training as a result of privacy incidents or potential privacy risks.

### *National Protection and Programs Directorate (NPPD)*

- Collaborated with the National Cybersecurity and Communications Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT) to provide cybersecurity information handling privacy training to 186 employees in the Office of Cybersecurity and Communications.
- Hosted the Office of Intelligence and Analysis (I&A) to brief 19 staff on Counterintelligence Awareness on May 13, 2015.
- Presented a briefing titled “Building Privacy Awareness” on June 9, 2015 at the Veterans Administration’s Privacy Symposium, and on August 19, 2015 at the IRS Privacy Council.
- Participated on a panel entitled, “The Relationship between Privacy and Records Management,” before the Federal Records Officer Network Meeting on July 21, 2015.
- Spoke to 58 attendees at an International Association of Privacy Professionals (IAPP) KnowledgeNet event on Designing Cyber Information Sharing with Privacy in Mind on September 15, 2015.
- Provided privacy and acquisitions refresher training on September 15, 2015 to a group of Contracting Officer Representatives (CORs) within the Office of Infrastructure Protection (IP), focusing on the implementation of the Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information.
- Hosted a panel discussion on September 16 & 17, 2015 regarding online safety entitled “Uh oh! Where did my data go? Tips on how to stay safe online” for 52 participants. The panel of NPPD cybersecurity experts discussed how the privacy risks continue to grow with the use of online banking, online shopping, social networking, and gaming.
- NPPD’s Office of Biometric Identity Management (OBIM) provided privacy awareness training to contractors onboarding for Homeland Advanced Recognition Technology in June 2015. OBIM also published two privacy tips in their internal newsletter/SharePoint website during this reporting period:
  - “Protect PII on Shared Drives” (published July 2015). This tip reminded individuals to add access controls around sites on shared drives that contain PII and SPII; and
  - “Your Phone Might Be Following You: 5 Tips to Protect Your Location-Based Privacy” (published September 2015). This tip reminded employees to review mobile app privacy policies because apps can collect PII and potentially share that data with third parties.

## *Science and Technology Directorate (S&T)*

- Conducted “Intros to S&T Privacy” for onboarding staff.
- Gave an overview of privacy issues with wearable technology to the S&T First Responders Group.

## *Transportation Security Administration (TSA)*

- Presented information via classroom training, web and phone conferencing on how to handle PII and the role of the Privacy Office to over 100 people, including TSA employees, cybersecurity groups, and staff at other federal agencies.
- Distributed a monthly newsletter, *Privacy Awareness Press*, to 420 employees.
- Conducted a seminar for 80 employees on privacy compliance documentation.
- Reached out to a variety of privacy and civil liberties groups and thought leaders to discuss TSA’s risk-based security, Pre-Check initiatives, and the Secure Flight program.

## *United States Citizenship and Immigration Services (USCIS)*

- Published a memo entitled “USCIS’ Commitment and Responsibility to Provide Privacy Protections” to reinforce to all personnel their commitment to protect privacy when using, sharing, collecting, storing and disposing of PII.
- Hosted the 5th Annual USCIS Privacy Awareness Day on September 2, 2015. This year’s theme was *Privacy-How to Protect Information*, and focused on what to do if you become a victim of a breach.
- Disseminated privacy awareness posters to raise awareness on protecting PII, storing and securing official records, and reporting privacy incidents.
- Published a public facing poster that promotes agency commitment to protecting the personal information of members of the public that has been entrusted to the agency.
- Hired a new Fraud Detection and National Security Directorate (FDNS) Privacy Advisor. The new advisor briefed employees on the mission of the new privacy program along with employees’ roles and responsibilities to ensure privacy is baked into FDNS activities.
  - Created a privacy tip series for publication in the FDNS bi-weekly newsletter to help raise privacy awareness.
  - Provided two separate training sessions on the privacy compliance process to members of the FDNS Program Management Office, Data Science and Screening Analytics Branch, and to the contractor staff supporting development of the Program Management Office’s Integrated Master Schedule.
- Conducted and completed 31 site visits and risk assessments of USCIS facilities. Provided insight and recommendations to leadership on findings/privacy risks, and how to improve privacy protections and awareness throughout each region.
- Briefed the Western Region District Directors on the USCIS Privacy Program and how they can promote privacy awareness within their office.
- Published the USCIS Office of Privacy quarterly newsletter entitled “Privacy Chronicles” to convey how to identify, report and mitigate privacy incidents.
- Published agency-wide privacy tips to highlight the appropriate use, access, sharing, and disposing of PII and how to effectively report a privacy incident.
- Hosted an instructor-led privacy training entitled *Safeguarding Sensitive PII*.

- Hosted instructor-led privacy training entitled *Understanding Privacy Incidents* to convey how to identify, report and mitigate privacy incidents.
- Updated the mandatory, annual online privacy training course entitled *USCIS Privacy Awareness Training* to add the general requirements for the operational use of social media.
- Updated the computer-based privacy training entitled *Privacy Requirements for Operational Use of Social Media 1.0*.
- Hosted “Privacy and Social Media” training for summer interns on June 18, 2015 to convey how to protect online personal information.
- Hosted training on the privacy compliance process entitled *Privacy Compliance Bootcamp* for the new Regional and District Privacy Officers on September 22, 2015.
- Hosted a high level briefing on the USCIS privacy compliance program for USCIS Senior Leadership at the extended leadership meeting on July 7, 2015.
- Hosted a briefing for the Forms Management Branch on the privacy compliance process on September 17, 2015.

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

- Provided privacy training, including an in-depth compliance session, to the CBP Component Privacy Liaisons.
- Presented at two Professionalism Service Managers Orientation trainings, providing privacy guidance and overall awareness of the CBP Privacy Office.
- Presented at the American Society of Access Professionals, National Training Conference, providing an in-depth presentation on mitigation and remediation of privacy incidents.
- Presented at the September 2015 meeting of DHS’ Data Integrity Privacy Awareness Committee.
- Supported computer based privacy training for 52,415 individuals.

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

- Trained the Office of Congressional Relations and the Office of the Principal Legal Advisor, Government Information Law Division, on general privacy concepts and disclosures to Congress under the Privacy Act.
- Trained the Homeland Security Investigations Office of Intelligence on April 10 and August 6, 2015, discussing disclosures under the Privacy Act, how to safeguard Sensitive PII, and how to report and mitigate privacy incidents.
- Provided privacy training to 100 new employees during the onboarding process.
- Conducted a Privacy Q&A with the Office of Public Affairs on June 23, 2015, to discuss the details and effective communications on the significant data breaches affecting federal personnel that occurred in 2014 and 2015.

### ***United States Secret Service***

- Provided privacy training to Headquarters staff and new Special Agent and Uniformed Division classes. The training explained how to safeguard PII, and how and where to report privacy incidents.
- Hosted a Privacy Awareness Day event entitled, “Don’t Put Privacy in Jeopardy,” on June 17, 2015, to educate employees and contractors about privacy best practices and federal privacy laws.

- Disseminated privacy compliance brochures and flyers on how to safeguard PII in an effort to promote privacy awareness.

## V. 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.<sup>19</sup>

Type of Complaint	Number of complaints received during the reporting period	Disposition of Complaint		
		Closed, Responsive Action Taken <sup>20</sup>	In Progress (Current Period)	In Progress (Prior Periods)
<b>Process &amp; Procedure</b>	10	9	2	4
<b>Redress</b>	307	306	1	0
<b>Operational</b>	1,209	1,177	60	4
<b>Referred</b>	47	47	0	0
<b>Total</b>	1,573	1,527	63	8

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.<sup>21</sup>
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.

<sup>19</sup> See DHS Privacy Policy Guidance Memorandum 2007-01, *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>.

<sup>20</sup> These totals include complaints opened and closed during this reporting period, and complaints opened in prior reporting periods but closed during this reporting period.

<sup>21</sup> 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.

4. **Referred:** The DHS Component or the Privacy Office 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 DHS Component or the Privacy Office 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 DHS Component or the Privacy Office 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:** The CBP INFO Center was contacted by a complainant who arrived at a Port of Entry and was referred for secondary examination. The complainant expressed concern about missing a flight connection due to the delay. The complainant alleged that the selection for secondary examination was the result of being targeted.

**DISPOSITION:** The CBP INFO Center responded to the complaint and explained CBP's search authority, the secondary process and its mission. In addition, CBP encouraged the complainant to speak with an on-site supervisor in the future to address any comments or concerns raised during the inspection process. CBP also stated that all allegations of unprofessional conduct by any CBP employees are taken seriously, and that CBP appreciated the complainant's initiative in bringing this matter to its attention.

**COMPLAINT:** The CBP INFO Center was contacted by the complainant who had been selected for random inspection upon arrival at a Port of Entry. The complainant alleged that the CBP Officer was rude, condescending, and asked inappropriate questions.

**DISPOSITION:** The CBP INFO Center researched the incident in CBP databases and responded directly to the complainant. The response explained CBP's mission, search authority, and the secondary process. In addition, CBP encouraged the complainant to speak with an on-site supervisor or Passenger Service Manager in the future to address any comments or concerns raised during the inspection process. CBP also stated that all allegations of unprofessional conduct by any CBP

employees are taken seriously, and that CBP appreciated the complainant's initiative in bringing this matter to its attention.

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

**COMPLAINT:** An ICE employee brought to ICE Privacy Office's attention that an ICE field office – in an attempt to compile emergency contact lists – was inadvertently emailing sensitive information, including name, Social Security Number (SSN), and medical information to several employees within the office who did not have a need to know.

**DISPOSITION:** ICE Privacy discussed the emergency contact list practices with field office management, and determined that the office does not need to collect SSNs in order to compile these specific emergency contact lists. To eliminate the possibility of emails being sent to those without a need to know, the office will now use access-restricted SharePoint to collect and track emergency contact list information.

## VI. CONCLUSION

As required by the 9/11 Commission Act, this second semiannual report for FY15 summarizes the Privacy Office's activities from April 1 – September, 30 2015. 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.