Department of Homeland Security

Privacy Office

Fiscal Year 2015 Semiannual Report to Congress

For the period October 1, 2014 – March 31, 2015

July 6, 2015

Homeland Security

Foreword

July 6, 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 October 1, 2014 – March 31, 2015.[1]

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[2] requires the DHS 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 DHS 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),[3] sets forth the responsibilities of the DHS Privacy Office. The mission of the DHS 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*,[4] the *Freedom of Information Act*,[5] and the *E-Government Act of 2002*,[6] 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.

[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. The DHS Privacy Office semiannual reports will cover the following time periods: April – September, and October – March.
[2] 42 U.S.C. § 2000ee-1(f).
[3] 6 U.S.C. § 142.
[4] 5 U.S.C. § 552a.
[5] 5 U.S.C. § 552.
[6] Pub. L. No. 107-347 (Dec. 17, 2002).

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

Sincerely,

Karen L. Neuman
Chief Privacy Officer
U.S. Department of Homeland Security

Pursuant to congressional notification requirements, the DHS 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

DHS PRIVACY OFFICE
FISCAL YEAR 2015
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 12
A. Privacy Training and Awareness 12
B. DHS Privacy Office Awareness & Outreach 14
C. Component Privacy Office Awareness & Outreach 16
V. PRIVACY COMPLAINTS AND DISPOSITIONS 19
VI. CONCLUSION 22

II. LEGISLATIVE LANGUAGE

Section 803 of the *9/11 Commission Act of 2007*,[7] 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,[8] 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."

[7] 42 U.S.C. § 2000ee-1.

[8] 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.

III. PRIVACY REVIEWS

The Department of Homeland Security (DHS or Department) Privacy Office (DHS Privacy Office or 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 through the Privacy Impact Assessment process;

2. Privacy Impact Assessments, as required under the *E-Government Act of 2002*,[9] the *Homeland Security Act of 2002*,[10] and DHS policy;

3. System of Records Notices, as required under the Privacy Act, and any associated Final Rules for Privacy Act exemptions;[11]

4. Privacy Act Statements, as required under the Privacy Act,[12] to provide notice to individuals at the point of collection;

5. Computer Matching Agreements, as required under the Privacy Act;[13]

6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*;[14]

7. Privacy Compliance Reviews, per the authority granted to the DHS Chief Privacy Officer by the *Homeland Security Act of 2002*;[15]

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.

[9] 44 U.S.C. § 3501 note.
[10] 6 U.S.C. § 142.
[11] 5 U.S.C. § 552a(j), (k).
[12] 5 U.S.C. § 552a(e)(3).
[13] 5 U.S.C. § 552a(o)-(u).
[14] 42 U.S.C. § 2000ee-3.
[15] 6 U.S.C. § 142.

Table I
Reviews Completed: *October 1, 2014 - March 31, 2015*

Type of Review	Number of Reviews
Privacy Threshold Analyses	334
Privacy Impact Assessments	19
System of Records Notices and associated Privacy Act Exemptions	20
Privacy Act (e)(3) Statements	6
Computer Matching Agreements	1
Data Mining Reports	0
Privacy Compliance Reviews	1
Privacy Reviews of IT and Program Budget Requests[16]	0
Other Privacy Reviews	0
Total Reviews	***381***

[16] The Chief Information Office prepares a privacy score once a year as part of its Office of Management and Budget Exhibit 300 reporting. Therefore, reviews for this category are calculated only once a year during the fourth quarter.

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 19 new, updated, or renewed PIAs. All published DHS PIAs are available on the DHS Privacy Office website, www.dhs.gov/privacy; we include a summary of key PIAs here, along with a hyperlink to the full text.

DHS/TSA/PIA-018(g) Secure Flight Program Update *(December 8, 2014)*
The Transportation Security Administration's (TSA) Secure Flight program screens aviation passengers and certain non-travelers before they access airport sterile areas or board aircraft. This PIA update reflects the incorporation of risk-based assessments generated by aircraft operators using data in their existing Computer-Assisted Passenger Prescreening Systems (CAPPS). CAPPS assessments are used in risk-based analysis of Secure Flight and other prescreening data that produce a boarding pass printing result for each passenger. In addition, this update reflects that Secure Flight now incorporates checks against watch lists of lost and stolen travel documents, including international passports. It also reflects the addition of records of TSA and DHS employees who have opted-in to TSA Pre-Check as another known traveler population stored by Secure Flight.

DHS/USCIS/PIA-013-01 Fraud Detection and National Security Directorate (FDNS) *(December 16, 2014)*
United States Citizenship and Immigration Service (USCIS) created FDNS to strengthen the integrity of the Nation's immigration system, and to ensure that immigration benefits are not granted to individuals who may pose a threat to national security and/or public safety. In addition, FDNS is responsible for detecting, deterring, and combating immigration benefit fraud. USCIS updated and reissued this PIA to include: (1) FDNS's sharing with law enforcement agencies; and (2) the DHS/USCIS/ICE/CBP-001-Alien File, Index and National File Tracking System of Records, published November 21, 3013 at 78 FR 69864, as coverage for initiatives under this PIA.

DHS/FEMA/PIA-034(a) Electronic Fingerprint System (EFS) *(January 8, 2015)*
The Federal Emergency Management Agency's (FEMA) Office of the Chief Security Officer uses EFS as part of the security suitability, clearance, and badging process for FEMA employees, contractors, and affiliates. FEMA updated the original PIA because EFS now uses NPPD's Office of Biometric Identity Management's (OBIM) Automated Biometric Identification System (IDENT) to store fingerprints as a part of its background investigations.

DHS/NPPD/PIA-020(a) Private Sector Clearance Program for Critical Infrastructure *(February 11, 2015)*
The Private Sector Clearance Program for Critical Infrastructure (PSCP), established in 2006, ensures that critical infrastructure private sector owners, operators, and industry representatives, specifically those in positions responsible for the protection, security, and resilience of their assets, are processed for the appropriate security clearances. National Protection and Programs Directorate (NPPD) updated this PIA to account for changes to the program since the publication of the original PIA on November 2, 2011, including eenhancements made to the PSCP to meet the intent of Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*.

DHS/ALL/PIA-046(b) DHS Data Framework *(February 27, 2015)*
The DHS Data Framework ("Framework") is a scalable information technology program with built-in capabilities to support advanced data architecture and governance processes. The Framework is DHS's "big data" solution to build in privacy protections while enabling more controlled, effective, and efficient use of existing homeland security-related information across the DHS enterprise, and with other U.S. Government partners, as appropriate. Currently, the Framework includes the Neptune and Cerberus systems and the Common Entity Index. Beginning in April 2015, DHS intends to mature the Framework during an Initial Operational Capability phase, which will include new DHS data sets, additional DHS users, and new technical capabilities (e.g., data refresh) for use within a controlled operational context. DHS updated the Framework PIA to reflect the transition to this Initial Operational Capability phase.

DHS/CBP/PIA-025 1:1 Facial Recognition Air Entry Pilot *(March 11, 2015)*
U.S. Customs and Border Protection (CBP) is conducting the 1:1 Facial Recognition Air Entry Pilot to allow CBP officers stationed at air ports of entry to use facial recognition technology to assist them in determining whether an individual presenting themselves with a valid United States electronic passport is the same individual photographed in that passport. The operational goals of this pilot are to determine if facial recognition technology can be incorporated into current CBP entry processing with acceptable impacts to processing time, while effectively providing the officers with a tool to reveal imposters. CBP issued this PIA to evaluate the privacy risks of using facial recognition software at an air port of entry.

DHS/ICE/PIA-039 Acquisition and Use of License Plate Reader Data from a Commercial Service *(March 19, 2015)*
United States Immigration and Customs Enforcement (ICE) uses information obtained from license plate readers (LPR) as one investigatory tool in support of its criminal investigations and civil immigration enforcement actions. Because LPR information can be combined with other data to identify individuals and, therefore, meets the definition of PII, ICE conducted this PIA to describe how it intends to procure the services of a commercial vendor of LPR information to expand the availability of this information to its law enforcement personnel. ICE is neither seeking to build nor contribute to a national public or private LPR database. In addition, through this PIA, ICE is assessing the potential impact of the use of information obtained from LPRs on the civil liberties of the public, and explaining the measures to be put in place to mitigate such concerns. ICE will publish an updated version of this PIA before the commercial solution described herein becomes operational.

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 DHS Privacy Office published 20 SORNs. 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 the DHS Privacy Office website, www.dhs.gov/privacy.

DHS/USCG-029 Notice of Arrival and Departure *(October 31, 2014)*
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 assists with assigning priorities for conducting maritime safety and security regulations. As a result of a biennial review of this system, the DHS/USCG updated this system of records notice to revise the system manager and address categories.

DHS/CBP-009 Electronic System for Travel Authorization (ESTA) *(November 4, 2014)*
This system of records allows the CBP to collect and maintain records on nonimmigrant aliens seeking to travel to the United States under the Visa Waiver Program, and other persons, including U.S. citizens and lawful permanent residents, whose names are provided to DHS as part of a nonimmigrant alien's ESTA application. This revised notice updated: (1) the categories of individuals covered by the system; and (2) categories of records in the system to include revised eligibility questions, and additional data elements collected on the ESTA application.

DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) *(December 1, 2014)*
This system allows ICE Homeland Security Investigations (HSI) to collect and maintain records for the purpose of enforcing criminal and civil laws pertaining to customs violations, including trade-based money laundering. This system of records was modified to: (1) update existing and add new categories of individuals; (2) clarify existing and add new categories of records; (3) reflect a proposed change to the retention period of the system's data; and (4) update the description of the record sources. The SORN was also updated to expand coverage to a new IT system called FALCON-Roadrunner.

DHS/TSA-019 Secure Flight Records *(January 5, 2015)*
This system of records allows the TSA to collect and maintain records on aviation passengers and certain non-travelers to screen such individuals before they access airport sterile areas or board aircraft, in order to identify and prevent a threat to aviation security or to the lives of passengers and others. TSA reissued this system of records to update the categories of records, to include records containing risk-based assessments generated by aircraft operators using data in their Computer-Assisted Passenger Prescreening Systems. This change identified additional passengers who may be eligible for expedited screening at airport security checkpoints.

C. Privacy Compliance Reviews

The DHS 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.

During the reporting period, the Office completed one PCR on the Enhanced Cybersecurity Services (ECS) Program:

Enhanced Cybersecurity Services (ECS) Program, April 9, 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 DHS Privacy Office 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.

Public PCR reports are available on the DHS Privacy Office website, www.dhs.gov/privacy, under "Investigations and Compliance Reviews."

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

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

Mandatory Online Training

104,819 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.

8,994 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 DHS Privacy Office-adjudicated Component Social Media Operational Use Template(s).

Classroom Training

4,546 DHS personnel attended instructor-led privacy training courses, including the following:

- **New Employee Training:** The DHS 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[17] also offer privacy training for new employees when they onboard. In addition, the DHS 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.

- **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 DHS 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 DHS 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 Office provides privacy training each month to participants of this week-long training program.

- **Reports Officer Certification Course**: The Office provides privacy training to reports officers who prepare intelligence reports as part of the DHS Intelligence Enterprise certification program.

[17] Ten DHS offices and components have a Privacy Officer.

- **Privacy Training for Fusion Centers**: The Office collaborates with the DHS 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 Office launched 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. DHS Privacy Office Awareness & Outreach

Publications

- In January 2015, the DHS Privacy Office published the *2014 Data Mining Report to Congress*. This report discusses activities currently deployed or under development at the Department that meet the *Data Mining Reporting Act's* definition of data mining, and provides the information set out in the Act's reporting requirements for data mining activities.

Meetings & Events

- Advocate Meeting – On October 14, the Chief Privacy Officer hosted a special meeting for privacy advocates with the DHS Assistant Secretary for Cybersecurity & Communications, who provided an overview of DHS's cybersecurity programs.

- Privacy Summit – On November 3, the Chief Information Officer Council Privacy Committee, which is co-chaired by the DHS Deputy Chief Privacy Officer, hosted a one-day workshop that convened budget, procurement, human resources, public affairs, congressional affairs, and intergovernmental affairs staff from DHS and other federal agencies in to discuss privacy and security. Subject matter experts shared best practices for protecting privacy, and ways to improve collaboration across the enterprise.

- Winter Technology Exchange – On December 2, 2014, the Deputy Chief Privacy Officer gave a presentation on DHS's privacy practices at this workshop sponsored by the Department of Health and Human Services.

- International Association of Privacy Professionals (IAPP), Practical Privacy Series – U.S. Government – On December 2, 2014, the Deputy Chief Privacy Officer moderated a panel presentation entitled, "*The Privacy Act at 40*." The panel presented the various strengths and weaknesses of the law, as well as lessons learned. Other panelists included senior practitioners from the Departments of Justice and Health and Human Services, the Social Security Administration, and the Office of the Director of National Intelligence.

- Government Technology Research Alliance (GTRA) Conference – On December 8, 2014, the Deputy Chief Privacy Officer spoke on privacy challenges as they relate to Big Data and cloud computing at this conference in Leesburg, Virginia.

- National Reconnaissance Office's (NRO) Privacy Symposium – On January 28, 2015, the Deputy Chief Privacy Officer gave the keynote address on privacy issues related to unmanned aircraft to kick-off the NRO's privacy awareness month.

- IAPP Global Privacy Summit – On March 6, 2015, the Chief Privacy Officer participated on a panel discussion entitled, "*The Job of Protecting Both the Nation's Security and Privacy*," in Washington, DC.

- International Workshop on National Security and Societal Implications of Remotely Piloted Airborne Vehicles and Related Technologies – On March 20, 2015, the Senior Advisor for Privacy and Intelligence spoke about unmanned aircraft privacy issues at the Center for Strategic and International Studies in Washington, DC.

- United States – European Union Data Protection and Privacy Agreement – The Chief Privacy Officer participated in the ongoing negotiations with the European Union on privacy standards for personal data shared in support of law enforcement and homeland security operations.

C. Component Privacy Office Awareness & Outreach

Federal Emergency Management Agency (FEMA)

- Hosted inter-agency meetings and workshops on a high profile DHS initiative for the Coast Guard, FEMA's Office of Chief Counsel Field Operations, and the Emergency Management Institutes.
- Conducted privacy training and site risk analysis in the National Capital Region to reinforce best practices for safeguarding PII, with an emphasis on securing PII during office relocations.
- Disseminated privacy fact sheets, posters, and other best practice materials to increase privacy awareness, enhance PII protection, and encourage the reporting and mitigation of privacy incidents.
- Participated in the Intranet Governance Working Group to establish governance around FEMA's use of SharePoint, specifically with respect to handling PII.

National Protection and Programs Directorate (NPPD)

- Moderated a panel entitled "The Why Behind Complex Privacy Controls" at the *Connect:ID Conference* on biometrics and identity management in Washington D.C., on March 25, 2015.
- Hosted a four-day *Privacy Training Days* event, March 16 - 19, 2015, attended by 274 employees and contractors in the National Capital Region.
- Provided cybersecurity information handling privacy training to 124 employees in the Office of Cybersecurity and Communications.
- Hosted a series of Counterintelligence Awareness Briefings on November 13 - 19, 2014.
- Hosted the annual NPPD Privacy and Technology Workshop on December 10, 2014, an interactive technology demo/fair presented by various NPPD program offices which allowed employees to learn exciting and informative details on topics including security, privacy, malware, and encryption.
- Created a new Privacy and Acquisitions Training Course for acquisitions professionals to learn NPPD's core privacy provisions, and how to determine when those provisions should be applied to statements of work.
- Created a new Social Media Requirements Training Course to provide an overview of privacy risks associated with the use of social media, as well as information on DHS's social media policy, including how to gain access, roles and responsibilities, and general rules of behavior for social media use.
- Distributed privacy tips via e-newsletters: (1) how to safeguard Sensitive PII within the SharePoint environment; (2) how to safeguard Sensitive PII during office moves; (3) reminder to lock your laptop and take your PIV credential with you when leaving their desk; and (4) remove all Sensitive PII from emails and place it in a password-protected or encrypted attachment.

Office of Health Affairs (OHA)

- Attended both the IAPP Global Privacy Summit in March 2015, in Washington, DC, and the CIO Council Privacy Committee's Privacy Summit on November 3, 2014, in Washington, DC.
- Distributed *The Daily Wrap* to all staff, an internal newsletter containing privacy-related information, including a *10 Step Guide to Privacy*.

Science and Technology Directorate (S&T)

- Presented to the USCIS Verification Office on privacy and the Internet of Things on October 7, 2014.
- Participated on a panel discussing unmanned aircraft and privacy at the Information Security and Privacy Advisory Board on October 23, 2014.
- Served as a panelist on *The Internet of Things: Privacy, Security, New Risks and Developing Threats*, at the American Conference Institute on January 15, 2015.
- Presented on Big Data and Privacy at the DHS Big Data Analytics Workshop on January 16, 2015.
- Presented to the National Reconnaissance Office on Privacy and Disruptive Technologies on January 28, 2015.
- Briefed the American Civil Liberties Union and the Electronic Privacy Information Center on the Air Entry Exit Reengineering Project on March 10, 2015.

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 10,000 people, including TSA employees, cybersecurity groups, and staff at other federal agencies.
- Sent a broadcast message about employee responsibilities for the safeguarding of Sensitive PII to 60,000 employees.
- Distributed a monthly newsletter, *Privacy Awareness Press*, to 70 employees.
- Trained 60 employees in the Office of Security Policy and Industry Engagement.

United States Citizenship and Immigration Services (USCIS)

- Trained records managers on ways to prevent privacy incidents by following agency policies for handling and safeguarding official records.
- Trained the Forms Management Branch on privacy requirements for the forms review process.
- Briefed the Office of Policy and Strategies on USCIS privacy policies, privacy compliance, how to safeguard PII, and requirements for Computer Readable Extracts (CREs).
- Participated in the Data Privacy Day on January 28, 2014, in the Northeast Region.
- Conducted a Virtual Privacy Chat with District offices to provide a high-level overview of privacy activities in the Federal Government.
- Implemented an external privacy awareness program to USCIS customers on how to protect their personal information during the immigration and benefit process.
- Audited program offices to ensure that employees and contractors are following agency policy to safeguard PII.
- Implemented an employee privacy awareness program that included posters, email tips, brochures, and events.
- Distributed a privacy newsletter to provide awareness on new privacy policies, guidance, upcoming privacy events, and privacy training.

United States Coast Guard (USCG)

- Participated in a panel discussion on privacy compliance at the 2015 Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, and Information Technology Strategic Summit held at the St. Elizabeth's complex. 200 personnel attended.
- Trained 14 staff on how to safeguard PII during office moves at the USCG Personnel Service Center, National Pollution Fund Center, and Coast Guard Investigative Service.
- Attended various training sponsored by the National Archives and Records Administration.

United State Customs and Border Protection (CBP)

- Attended the IAPP Global Privacy Summit in March 2015, in Washington, DC.
- Issued a new internal Directive designed to address privacy policy, compliance, and implementation.
- Created a new Social Media Requirements Training Course to provide an overview of privacy risks associated with the use of social media, as well as information on DHS's social media policy, including how to gain access, roles and responsibilities, and general rules of behavior for social media use.
- Hired eight new privacy compliance specialists.

United States Immigration and Customs Enforcement (ICE)

- Trained 15 public hotline operators at the ICE Enforcement and Removal Operations Custody Programs privacy training on November 17, 2014.
- Trained the ICE Homeland Security Investigations Office of Intelligence on January 15, 2015, discussing disclosures under the Privacy Act, how to safeguard Sensitive PII, and how to report and mitigate privacy incidents.
- Provided training on privacy and the procurement process to contracting officers, contracting officer representatives, contract specialists, program managers, and mission support staff on January 29, 2015.

United States Secret Service

- Provided privacy overview training to new hires at bi-weekly employee orientation.
- Conducted Privacy Best Practice training on February 3, 2015 for Special Agents in Charge of the Investigative Issues Focus Group.
- Created and launched a new Operational Use of Social Media Training Course to provide employees with the privacy rules of behavior to follow when using social media for law enforcement purposes.
- Disseminated privacy awareness materials and posted information on privacy incidents and privacy complaints on the intranet to encourage employees to report and mitigate privacy violations.

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 DHS 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.[18]

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[19]	In Progress (Current Period)	In Progress (Prior Periods)
Process & Procedure	9	8	1	2
Redress	3	2	1	0
Operational	939	969	29	6
Referred	32	32	0	0
Total	983	1,011	31	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.[20]
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.

[18] *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).
[19] These totals include complaints opened and closed during this reporting period, and complaints opened in prior reporting periods but closed during this reporting period.
[20] 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 DHS 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 DHS Privacy Office refers to the proper agency.

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

1. *Closed, Responsive Action Taken*: The DHS Component or the DHS 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 DHS 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:

Transportation Security Administration (TSA)

Complaint: A traveler complained that he was unlawfully denied entrance to an airport, and detained by TSA personnel. The traveler presented identification documents that he had created himself. TSA did not accept his identification documents as valid, and offered to verify his identity using TSA processes. The traveler refused to participate, and, instead, demanded that TSA contact un-named individuals within the FBI to verify his identity. The traveler also refused to provide additional identification or information, claiming that TSA lacked authority over his travel, and the process was unconstitutional.

Disposition: TSA Privacy confirmed that appropriate screening procedures were followed, provided the traveler with a link to TSA information on acceptable identification documents, and encouraged his use of the identity verification process during future travel.

United States Customs and Border Protection (CBP)

Complaint: The CBP INFO Center was contacted by a complainant who stated that he was required to answer numerous questions, including questions directed to the complainant's spouse, resulting in the CBP Officer speaking sharply at the complainant's spouse. The complainant believed that the questions were unnecessary, and that CBP Officers should not ask numerous questions, nor treat American citizens as terrorists.

Disposition: The CBP INFO Center researched the incident in CBP databases and determined there were no records referring the traveler to secondary. The questions that were the subject of the complaint took place in primary. The CBP INFO Center responded to the complainant, explaining CBP search authority and the customary response for any perceived rude and unprofessional behavior.

Complaint: The CBP INFO Center was contacted by a complainant who arrived at a Port of Entry requesting admission into the United States, and was referred for a secondary examination. The complainant alleged that, during the examination, the CBP Officer was rude and unprofessional.

Disposition: The CBP INFO Center referred the complaint to the Office of Field Operations, which responded and explained CBP's mission, search authority, and the secondary process. In addition, CBP included information on the opportunity to speak with a supervisor to address any comments or concerns raised during the inspection process, and noted that all allegations of unprofessional conduct by CBP employees are taken seriously. CBP expressed appreciation for the complainant's initiative in bringing this matter to CBP's attention, and the Field Office provided guidance to the Port of Entry Officers to ensure that all travelers are treated in a professional manner.

United States Immigration and Customs Enforcement (ICE)

Complaint: ICE Privacy received a complaint from a union representative regarding the inclusion of Alien Registration Numbers (A-numbers) on employees' Administratively Uncontrollable Overtime (AUO) payroll timesheets in order to monitor compliance with AUO as required by law and policy. The union representative noted the limitations on the use of Sensitive PII, and questioned whether including A-numbers on timesheets would result in the A-number being shared with individuals who do not have a need to know.

Disposition: ICE Privacy coordinated with the ICE Office of the Principal Legal Advisor to determine that the use of A-numbers to properly account for AUO is acceptable. ICE Privacy responded to the union representative, advising that (1) while A-numbers are sensitive information, ICE timekeeping records already maintain many sensitive data elements about ICE personnel and are properly secured; and (2) the use of A-numbers only and no other alien-related identifying data in this instance is administratively appropriate, and does not pose an undue risk of harm to the alien.

VI. CONCLUSION

As required by the 9/11 Commission Act, this semiannual report summarizes the DHS Privacy Office's activities from October 1, 2014 – March 31, 2015. The DHS 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.