Department of Homeland Security

Privacy Office

Fiscal Year 2014 Semiannual Report to Congress

January 2015

Homeland Security

Foreword

January 5, 2015

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's *Fiscal Year 2014 Semiannual Report to Congress*, covering the time period March 1, 2014 – September 30, 2014.[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 30, and October – March. However, to avoid a data lapse from the prior report, which covered the period from December 2013 – February 2014, this initial semiannual report covers the time period March 1 – September 30, 2014.
[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).

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 C. A. Dutch Ruppersberger
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

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

DHS PRIVACY OFFICE
FISCAL YEAR 2014
SEMIANNUAL
SECTION 803 REPORT TO CONGRESS

Table of Contents

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 DHS Privacy Office activities:

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: *March 1 – September 30, 2014*

Type of Review	Number of Reviews
Privacy Threshold Analyses	332
Privacy Impact Assessments	30
System of Records Notices and Associated Privacy Act Exemptions	10
Privacy Act (e)(3) Statements	0
Computer Matching Agreements	6
Data Mining Reports	0
Privacy Compliance Reviews	1
Privacy Reviews of IT and Program Budget Requests[16]	111
Other Privacy Reviews	0
Total Reviews	***490***

[16] This reflects the total number of reviews for the year. 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 28 new, updated, or renewed PIAs, including PIA appendix updates. Since all published DHS PIAs are available on the DHS Privacy Office website, www.dhs.gov/privacy, we only include a summary of key PIAs here, along with a hyperlink to the full text.

DHS/CBP/PIA-024 Arrival and Departure Information System (ADIS) - Information Sharing Update (*March 7, 2014*)
U. S. Customs and Border Protection (CBP) updated the ADIS PIA to provide notice of a change in the National Counterterrorism Center's (NCTC) temporary retention of ADIS information to three years for U.S. Person information, and 10 years for non-U.S. Person information due to the March 2012 approval of *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Data sets Containing Non-Terrorism Information (2012 NCTC AG Guidelines).*

DHS/USCIS/PIA-013(a) Fraud Detection and National Security Directorate (*March 19, 2014*)
United States Citizenship and Immigration Services (USCIS) created the Fraud Detection and National Security (FDNS) Directorate 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 conducted this PIA to document and assess how FDNS collects, uses, and maintains PII.

DHS/TSA/PIA-042 TSA OIA Technology Infrastructure Modernization Program *(March 26, 2014)*
The Transportation Security Administration's (TSA) Office of Intelligence and Analysis (OIA) Technology Infrastructure Modernization (TIM) Program is an enterprise architecture designed to align TSA security threat assessment (STA) with credentialing activities for individuals. These individuals require access to transportation facilities, infrastructure, assets, Sensitive Security Information (SSI), or related security credentials or clearances. TIM integrates several vetting programs and systems and facilitates STA adjudication, credentialing, and redress processes. TIM accesses the same PII that is already collected for the underlying STA programs. TIM performs credentialing activities utilizing the PII that the underlying programs collect for the STAs. In light of this new information technology framework involving existing PII, TSA conducted this PIA.

DHS/ICE/PIA-015(f) Enforcement Integrated Database (EID) (*April 8, 2014*)
EID is a DHS shared common database repository for several DHS law enforcement and homeland security applications. EID captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations, and operations conducted by certain DHS components, namely United States Immigration and Customs Enforcement (ICE) and CBP. The original PIA for EID was published in January 2010. Since its publication, the PIA has been updated several times to reflect the expansion of information entered into EID, the types of information shared with foreign governments, and an enhanced electronic sharing capability. This EID PIA Update addresses the expansion of criminal history information sharing, which will include fingerprints and photographs, with foreign countries about their nationals who are being removed from the United States. The sharing of criminal history information is formalized by a Memorandum of Cooperation signed by DHS and each country that elects to participate in these sharing agreements.

DHS/NPPD/PIA-018(a) Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program (*May 20, 2014*)
The National Protection and Programs Directorate (NPPD) updated the CFATS Personnel Surety Program's PIA to account for changes to the program since the publication of the program's original PIA on May 4, 2011. On October 4, 2006, the President signed the *Department of Homeland Security Appropriations Act, 2007*. Section 550 requires DHS to regulate the security of high-risk chemical facilities, and also requires that DHS establish risk-based performance standards (RBPS) for high-risk chemical facilities. DHS promulgated 18 RBPS under CFATS. RBPS 12 – Personnel Surety – requires high-risk chemical facilities to: perform appropriate background checks on and ensure appropriate credentials for facility personnel, and, as appropriate, for unescorted visitors with access to restricted areas or critical assets, including, (i) measures designed to verify and validate identity; (ii) measures designed to check criminal history; (iii) measures designed to verify and validate legal authorization to work; and (iv) measures designed to identify people with terrorist ties.

DHS/S&T/PIA-028 Air Entry/Exit Re-engineering (AEER) (*May 28, 2014*)
The United States Congress mandated that the Secretary of Homeland Security implement a biometric verification system to monitor the arrival and departure of foreign nationals entering and departing the country. The Secretary, in turn, directed CBP and the Science and Technology Directorate (S&T) to test various biometric verification systems for effectiveness and efficiency. This PIA addresses the privacy risks and mitigation strategies associated with the testing phase of the AEER Project.

DHS/ALL/PIA-046(a) DHS Data Framework *(August 29, 2014)*
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. Currently, the Framework includes the Neptune and Cerberus systems, and the Common Entity Index. Between November 2013 and August 2014, DHS deployed a pilot/prototype to test different capabilities needed to implement the Framework. After the successful completion of the pilot/prototype phase, DHS now intends to mature the Framework by entering into the next phase—limited production capability. DHS updated the original Framework PIA to reflect this transition to limited production capability.

DHS/CBP/PIA-022 Border Surveillance Systems *(August 29, 2014)*
CBP's Border Surveillance Systems (BSS) are a combination of surveillance systems deployed to provide comprehensive situational awareness along the United States border to assist CBP in detecting, identifying, apprehending, and removing individuals entering the United States illegally. BSS includes commercially available technologies such as fixed and mobile video surveillance systems, range finders, thermal imaging devices, radar, ground sensors, and radio frequency sensors. CBP conducted this PIA because BSS collects and processes PII, including video images, photographs, radio frequency emissions, and location information.

DHS-ALL-PIA-045 Loaned Executive Program *(September 29, 2014)*
DHS's Private Sector Office manages the Department-wide Loaned Executive Program (LEP). LEP is a special unpaid opportunity for executive-level private sector, academic, and cyber security experts to share their expertise with DHS. Through LEP, DHS seeks innovative solutions to its homeland security challenges. DHS conducted this PIA because LEP collects PII from members of the public.

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 ten SORNs and two Final Rules for Privacy Act Exemptions. These documents are summarized below, and a hyperlink to the *Federal Register Notice* is included. 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.

SORNS

DHS/FEMA-009 Hazard Mitigation, Disaster Public Assistance and Loans Program (*March 24, 2014*)
The Federal Emergency Management Agency (FEMA) updated this system of records to include all disaster-related grant and loan programs, including public assistance programs, and renamed the system of records as stated above to reflect the changes. The consolidated and updated DHS/FEMA-009 provides notice of FEMA's collection and maintenance of records from points of contact from states, tribes, local governments, and other entities applying for all grant money programs through FEMA's public assistance grants program, disaster loan program, and the Hazard Mitigation Assistance grant programs. This system of records also allows information collection from individuals who may receive public assistance through these grants.

DHS/USCG-024 United States Coast Guard (USCG) Auxiliary Database (*April 3, 2014*)
This system of records allows the USCG to track and report contact, activity, performance, and achievement information about members of its volunteer workforce element, the USCG Auxiliary.

DHS/ALL-020 Internal Affairs System of Records (*April 28, 2014*)
This system collects and maintains records related to investigations, including allegations of misconduct, resultant investigations conducted by DHS Headquarters or its Components, and any of the individuals involved in such investigations, with the exception of records of investigations conducted by the Office of the Inspector General. This revised notice includes several changes necessitated by the issuance of a final rule entitled *Standards To Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities* (6 CFR part 115), and to better reflect DHS's internal affairs records systems.

DHS/FEMA-003 National Flood Insurance Program Files System of Records (*May 19, 2014*)
This system of records allows FEMA to collect and maintain records and information regarding applicants, policyholders, prospective policyholders, insurance agents, and other individuals associated with the National Flood Insurance Program (NFIP). FEMA needs the information in order to properly administer NFIP, which collects and maintains records of individuals that seek NFIP policies and/or rate quotes, apply for a NFIP policy, make NFIP insurance claims, appeal flood insurance claim decisions, and are involved in NFIP administration or marketing efforts.

DHS/NPPD-002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program (*May 19, 2014*)
This system of records allows NPPD to collect and maintain records on individuals–facility personnel and unescorted visitors–who have or are seeking access to restricted areas and critical assets at high-risk chemical facilities, and compare this information to the Terrorist Screening Database, the terrorist watchlist maintained by the Federal Bureau of Investigation's Terrorist Screening Center.

FINAL RULES

DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records Final Rule *(April 2, 2014)*
The Department of Homeland Security issued a final rule to amend its regulations to exempt portions of the Department of Homeland Security/U.S. Immigration and Customs Enforcement--014 Homeland Security Investigations Forensic Laboratory System of Records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. This system of records allows ICE to collect and maintain records by the Homeland Security Investigations Forensic Laboratory (HSI-FL). HSI-FL is a U.S. crime laboratory specializing in scientific authentication; forensic examination; research, analysis, and training related to travel and identity documents; latent and patent finger and palm prints; and audio and video files in support of law enforcement investigations and activities by DHS and other agencies.

DHS/NPPD-002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program Final Rule (*May 21, 2014*)
The Department of Homeland Security issued a final rule to amend its regulations to exempt portions of a newly established system of records titled, Department of Homeland Security/National Protection and Programs Directorate--002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program System of Records, from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. This system of records is discussed above.

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 April 16, 2014, DHS published the sixth PCR on the Office of Operations Coordination and Planning National Operations Center's (OPS/NOC) Publicly Available Media Monitoring and Situational Awareness Initiative. Since the initial PIA was published in June 2010, PCRs have been conducted bi-annually. The DHS Privacy Office conducted this sixth PCR to assess compliance with both the April 2013 PIA Update and the February 2011 SORN. The Office found OPS/NOC to be in compliance with the privacy requirements identified in both of these documents, and specific findings are discussed in the full review.

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

137,653 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.

13,003 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

5,110 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 explains how to document the FOIA records search, and how to complete the FOIA search form. The program is tailored to those 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.

- **Chief Human Capital Office Staff Training**: DHS Privacy Office staff provided classroom training on best practices for safeguarding Sensitive PII to over 200 members of the DHS Headquarters Office of the Chief Human Capital Officer in six sessions.

B. DHS Privacy Office Awareness & Outreach

Staff Awareness

The DHS Privacy Office disseminated a customizable tip sheet entitled *What You Need to Know About E-mailing Sensitive Personally Identifiable Information (SPII)* to all PPOCs. This customizable tip sheet was intended to be distributed to DHS staff as a reminder of their responsibilities to protect SPII when e-mailing within and outside of the DHS network.

Publications

1. On April 10, 2014, the DHS Privacy Office and Office for Civil Rights and Civil Liberties (CRCL) issued the first annual *Privacy and Civil Liberties Assessment Report*, which the offices compiled pursuant to Section 5 of Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity (Feb. 12, 2013). The report includes both office's assessments of certain DHS activities under Section 4 of the EO, as well as assessments conducted independently by the Departments of Treasury, Defense, Justice, Commerce, Health and Human Services, Transportation, and Energy, and by the Office of the Director of National Intelligence, and the General Services Administration. The report is posted on the DHS Privacy Office website.

2. On April 11, 2014, the *2014 Chief Freedom of Information Act (FOIA) Officer Report to the Attorney General* was posted on the DHS Privacy Office website. This report discusses actions taken by the Department to apply the presumption of openness, and to ensure that DHS has an effective system for responding to FOIA requests, increase proactive disclosures, fully utilize technology, reduce backlogs, and improve response times.

3. On September 30, 2014, the DHS Privacy Office published its *Annual Report to Congress*, highlighting the Office's accomplishments from June 2013 through July 2014.

Meetings & Events

- IAPP Global Privacy Summit – On March 6, 2014, the Chief Privacy Officer participated on a panel presentation entitled, "Protecting Privacy under the Cybersecurity Microscope," at this conference held in Washington, DC.

- Senate Homeland Security and Governmental Affairs (HSGAC) Briefing – On March 12, 2014, the Chief Privacy Officer briefed staff members of the HSGAC on the Privacy Office's Fiscal Year (FY) 2015 budget request.

- Senate Appropriations Committee Briefing – On March 19, 2014, the Chief Privacy Officer briefed staff members on the Privacy Office's FY 2015 budget request.

- Five Country Conference (FCC) Privacy and Informed Consent Working Group – On March 27, 2014, DHS Privacy Office staff represented DHS on a coordination call of the FCC Privacy Working Group. The Group was formed to analyze existing privacy and information sharing law among the FCC, identify impediments to sharing consistent with goals established by the Heads of Delegation, and recommend solutions.

- Privacy Coalition Meeting – On April 25, 2014, the Chief Privacy Officer met with privacy advocates to discuss the Office's 2014 priorities.

- Seventh Annual Training Conference of the American Society of Access Professionals (ASAP) – On May 14, 2014, the Deputy Chief Privacy Officer participated in a panel discussion entitled "Privacy Issues – Ask the Experts." In addition, the Associate Director of Communications co-led a session entitled "Creating a Culture of Privacy: Privacy Training and Awareness."

- Privacy Office Decade of Excellence Celebration – On May 14, 2014, the Chief Privacy Officer hosted an event commemorating a "Decade of Excellence" for the Privacy Office. The program recognized the major achievements of the privacy and FOIA staff in the Privacy Office, as well as the important work of the Privacy Officers and Privacy Points of Contact in the Components during the first decade of the Privacy Office. The Deputy Secretary addressed over 100 guests, including current and former DHS privacy and FOIA staff, former Chief Privacy Officers, representatives from the White House, the DHS Data Privacy and Integrity Advisory Committee, the Privacy and Civil Liberties Oversight Board, and privacy advocates.

- Data Protection and Privacy Agreement (DPPA) Plenary Session – On May 22 - 23, 2014, in Brussels, Belgium, the Chief Privacy Officer participated in a negotiation session of the DPPA along with several other DHS staff members.

- Privacy Office Annual Privacy Workshop – On June 10, the DHS Privacy Office hosted its annual workshop in Washington, D.C. Agenda topics included privacy compliance, identity management, and privacy training and awareness best practices. 160 people from over 40 federal agencies attended.

- Federal CIO Boot Camp – On June 18, the Deputy Chief Privacy Officer addressed an audience of federal chief information officers (CIO) on how to partner with your privacy office at the 2014 Federal CIO Boot Camp in Washington, DC.

- Government Technology Research Alliance Council Meeting – On June 23, the Deputy Chief Privacy Officer delivered remarks as part of a keynote panel presentation titled: *Is Widespread Big Data Adoption Here? Who's Using it, How, and What it Means for You*.

- National Governor's Association's State Cybersecurity Advisory Council Meeting – On July 23, the Deputy Chief Privacy Officer presented best practices for establishing a federal privacy office to federal, state, and private sector council members at a virtual meeting.

- Data Privacy and Integrity Advisory Committee Meeting – On September 22, the Privacy Office held a public meeting of the Data Privacy and Integrity Advisory Committee (DPIAC), both online and in-person in Washington, DC. The Chief Privacy Officer briefed Committee members on Privacy Office activities since the last meeting on January 30, 2014, and welcomed six new members appointed by the Secretary in May 2014. Participants were given an overview of DHS cybersecurity activities, and the implementation of the DHS Data Framework. Committee members voted on their recommendations to improve transparency and oversight of the DHS Data Framework.

C. Component Privacy Office Awareness & Outreach

Federal Emergency Management Agency (FEMA)

- Initiated a National Capital Region-wide privacy training and site risk analysis campaign in support of the agency's Workplace Transformation Initiative to reinforce best practices for securing PII during office relocations, and ensuring PII protection in an open work environment.
- Developed a Privacy Compliance Foundations training module and presented it to Information System Security Officers (ISSOs), Information System Security Managers (ISSMs), System Owners, Program/Project Managers, and attorneys across FEMA's program offices, Regional Offices, and National Processing Service Centers. The goal is to enhance the quality of privacy compliance documents submitted by these professionals, limit review iterations, and expedite the clearance and approval process.
- Continued to disseminate privacy fact sheets, posters, and broadcast e-mail messages to highlight best practices for protecting PII and reporting and mitigating privacy incidents.

National Protection and Programs Directorate (NPPD)

- Issued guidance on procedures for making contact with industry and service providers to ensure that procurement operating procedures are followed and PII and other sensitive data remain protected throughout the procurement process.
- Attended a one-day training seminar on virtual classroom development and presentation at the Federal Law Enforcement Training Center, with a goal of creating webinar based information law-related training modules for Federal Protective Service (FPS) personnel located throughout the United States and its territories.
- Participated in an informal meeting with the Privacy and Civil Liberties Oversight Board, hosted by the DHS Office for Civil Rights and Civil Liberties, to provide an overview of the Department's cybersecurity activities and oversight on August 14, 2014. NPPD's Under Secretary and Assistant Secretary for Cybersecurity & Communications delivered remarks and shared in a discussion regarding compliance best practices to consider in automated cybersecurity information sharing systems.
- Provided a DHS Cybersecurity Overview to the DPIAC by the Assistant Secretary for Cybersecurity & Communications on September 22, 2014.
- Provided various program updates to the DPIAC Cyber Subcommittee, and discussed the continuous evaluation of DHS's technical and policy approach to cybersecurity initiatives on September 23, 2014.
- Created a secure print privacy tip with instructions on how to use the secure print feature to safeguard documents while printing.

NPPD Privacy also conducted privacy training:

- Hosted a two-day *Privacy Training Days* event, with sessions held at four directorate office locations, targeting employees and contractors in the National Capital Region in March 2014. All 128 attendees received credit for completing their annual privacy training requirement.
- Provided a specialized privacy briefing to 103 employees and contractors of the FPS Personnel Security Division in March 2014.
- Provided a privacy overview training to 18 Office of Infrastructure Protection, Infrastructure Security Compliance Division chemical inspectors in April 2014.

- Co-hosted a training webinar with CRCL for 73 staff in the Office of Infrastructure Protection Protective Security Advisors (PSAs) on privacy, civil rights and civil liberties considerations that employees and contractors should be aware of when developing and reviewing external products.
- Provided a virtual privacy briefing to 140 regional division directors and staff in FPS Resource Management on May 1, 2014.
- Provided a Privacy 101 briefing to 15 employees and contractors of the Office of Infrastructure Protection, Infrastructure Security Compliance Division Mission Support Branch on May 14, 2014.
- Participated in the DHS Privacy Workshop in June 2014 by leading break-out teams for an interactive privacy compliance walkthrough focused on applying recently learned privacy compliance principles to adjudicating a PTA.
- Provided four training sessions on cybersecurity information handling training to 86 employees in the Office of Cybersecurity and Communications.
- Hosted guest speakers from the Federal Trade Commission on September 24, 2014 to discuss the basics on identity theft: what is identity theft, how you can protect yourself, and how you can resolve identity theft problems.

Science and Technology Directorate (S&T)

The S&T Privacy Officer presented at the following events:

- S&T's Developing Solutions for Better Practices in Data Sharing Workshop, presentation on *Building Privacy into Research Projects*, March 2014.
- Department of Veterans Affairs Privacy Awareness Week, April 2014.
- Netherlands Bilateral Science & Technology Delegation, May 2014.
- DHS Privacy Workshop, June 2014.
- S&T's Industry Day: *Data Privacy Technologies Research and Developmen*t, June 2014.
- USCIS's Disruptive Technologies and Privacy Workshop, July 2014.
- Privacy and Information Security Incidents Webinar at S&T, September 2014
- In-Q-Tel presentation on Building Privacy into Research Projects, September 2014
- S&T Big Data Workshop, presentation on *Big Data & Privacy*, September 2014.

Transportation Security Administration (TSA)

- Presented information via web and phone conferencing on how to handle PII, and the role of the Privacy Office to over 2,600 people, including TSA employees, cybersecurity groups, and staff at other federal agencies.
- Sent a broadcast message about site administrator responsibilities for handling Sensitive PII on iShare to 521 employees.
- Distributed a monthly newsletter, *Privacy Awareness Press*, to approximately 70 employees.
- Developed and presented a training series to various TSA Offices on how to address agency requests for Secure Flight Data. Sent a broadcast message to the all 350 TSA Assistant Federal Security Directors for Law Enforcement (AFSD-LE).

United States Citizenship and Immigration Services (USCIS)

- Hosted the Fourth Annual Privacy USCIS Awareness Week. Events included a shared drive clean-up, privacy skits, and privacy awareness training. Featured guest speakers represented Hyundai Capital, Nokia's Compliance & Technology Office, and the DHS Office of the Chief Security Officer.
- Organized an agency-wide Information Sharing Working Group to address privacy risks associated with information sharing agreements.
- Conducted privacy awareness classroom training for the National Congressional Affairs Training Conference.
- Created the *Privacy Corner* article series for a monthly staff e-newsletter to promote privacy best practices.
- Conducted Privacy Compliance Boot Camp training for a new detailee to the USCIS Office of Privacy, providing guidance on how to complete privacy compliance documentation.
- Published multiple Privacy Tips on the USCIS intranet, highlighting best practices on the appropriate use, access, sharing and disposing of PII, and how to effectively report a privacy incident.
- Completed 12 site visits and risk assessments of USCIS facilities. Provided insight and recommendations to leadership on how to improve privacy protections and awareness throughout each region.
- Presented on a panel at the DHS Privacy Office Workshop entitled "*Identity Management for Government Privacy Professionals,*" along with senior officials from the General Services Administration and the Social Security Administration.
- Attended the *Federal Computer Week* seminar on *Identity Proofing for Effective Government Operations* on August 12, 2014.
- Attended the Safeguarding Health Information: Building Assurance through HIPAA Security Conference on September 23 – 24, 2014.

United States Coast Guard (USCG)

- Facilitated PTA New Template Training to over 25 staff members of the USCG Office of Standard Evaluation and Development.

United States Immigration and Customs Enforcement (ICE)

- Presented at the ICE Homeland Security Investigations, Office of Intelligence Basic Intelligence Training Course on April 2 and August 14, 2014, discussing disclosures under the Privacy Act, proper handling of Sensitive PII, and privacy incidents.

United States Secret Service (USSS)

- Hosted a Privacy Awareness Day event entitled, "Don't Put Privacy in Jeopardy," on June 24, 2014, to educate employees and contractors about privacy best practices, federal privacy laws, and historical events related to privacy.
- Conducted a presentation on safeguarding PII on July 23, 2014, to USSS Administrative Officers.
- Posted privacy awareness posters and flyers to encourage staff to safeguard PII.
- 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 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	14	15	1	1
Redress	0	0	0	0
Operational	1581	1604	55	6
Referred	15	16	0	0
Total	***1610***	***1635***	***56***	***7***

.

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

Complaint: The complainant contacted the TSA Privacy Office via email that she was advised by an airline to open the lock on her luggage when she checked-in for her flight.

Disposition: The TSA Privacy Office responded, explaining that if her luggage contents caused an alarm, TSA would break the lock to inspect the contents. The TSA Privacy Office also explained that the complainant could not remain with her luggage after check-in because the inspection would not occur in a public area. The complainant thanked the TSA Privacy Office for the information.

U. S. Customs and Border Protection

Complaint 1: The CBP INFO Center was contacted by a complainant about treatment at a Port of Entry. The complainant reported that she was referred to secondary, handcuffed, and her pet was temporarily taken away. The complainant stated that, while in secondary, she was strip searched and then admitted to the United States. The complainant advised CBP INFO Center that she "was extremely angry and upset with the process," and alleged that the secondary search was a violation of her constitutional rights.

***Disposition*:** The CBP INFO Center researched the incident in CBP databases and confirmed that the complainant had been referred to secondary. The CBP INFO Center could not substantiate the complainant's claim that her constitutional rights had been violated after a review of the secondary record did not find CBP Office misconduct or unprofessionalism. The CBP INFO Center advised the complainant of CBP's border search authority and explained that secondary searches are within CBP's search authority.

Complaint 2: The CBP INFO Center was contacted by a complainant concerning his experience when requesting admission to the United States at a Port of Entry. The complainant stated that the CBP Officer at the border asked to examine his cell phone and requested the passcode. The complainant acknowledged that he was reluctant to allow the officer to examine his phone, but was advised that he was required to unlock the cell phone for examination or the phone would be impounded. The complainant unlocked the telephone and handed it to the CBP Officer, who "searched" through the cell phone. Complainant states that this search was performed in violation of CBP Directive No. 3340-049, 5.1.3, Searches of Electronic Devices, because the search was "not conducted in the presence of a supervisor."

***Disposition*:** The CBP INFO Center responded to the complainant via email to clarify that the referenced directive does not require 100 percent supervisor presence. The CBP INFO Center noted that the referenced section of the Directive states: "Searches of electronic devices will be documented in appropriate CBP system of records, and should be conducted in the presence of a supervisor. In circumstances where operational considerations prevent a supervisor from remaining present for the entire search, or where a supervisor presence is not practicable, the examining officer shall, as soon as possible, notify the appropriate supervisor about the search and any results thereof." The CBP INFO Center consulted the records and confirmed that the supervising officer was later notified that the complainant's mobile device was searched, and conveyed to the complainant that the proper procedure was followed.

Complaint 3: The CBP INFO Center was contacted by a complainant who was unable to retrieve his I-94 number from the CBP website after several attempts. The complainant arrived at a Port of Entry and the CBP Officer entered the information into the database using an incorrect surname. The complainant contacted CBP and was referred to the CBP Deferred Inspection Site at the Port of Entry to correct the database error.

***Disposition*:** The CBP INFO Center researched the incident and determined that the complainant's surname was still incorrectly entered in the CBP database. On behalf of the complainant, the CBP INFO Center contacted a CBP Officer at the Port of Entry who corrected the surname in the CBP database, and then sent a response to the complainant advising the situation was resolved.

VI. CONCLUSION

As required by the 9/11 Commission Act, this semiannual report summarizes the DHS Privacy Office's activities from March 1 – September 30, 2014. 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.