Department of Homeland Security

Privacy Office

2014 Annual Report to Congress

September 30, 2014

Homeland Security

Message from the Chief Privacy Officer

September 30, 2014

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *2014 Annual Report to Congress*, highlighting the achievements of the Privacy Office for the period July 2013 - June 2014.

On May 14, 2014, I hosted an event commemorating a "Decade of Excellence" for the Privacy Office. The program recognized the many major achievements of the privacy and *Freedom of Information Act* staff, as well as, the important work of their counterparts in the Components during the first decade of the Privacy Office.

DHS Deputy Secretary Alejandro Mayorkas addressed more than 100 guests, including current and former DHS privacy and *Freedom of Information Act* 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. The Deputy Secretary said, "Over the past decade, you have ensured that privacy protections are firmly embedded into the lifecycle of Homeland Security programs and systems. I am grateful for the contributions all of you have made to our missions. We are a stronger and more effective Department because of your hard work."

Expanding on the Deputy Secretary's observations, I am using this opportunity to recognize the privacy and *Freedom of Information Act* staff in my office and throughout the Department for their exceptional service.

Their jobs are profoundly important: the work they do every day influences the way our government responds to a complex range of threats. They ask the important, tough questions—with limited resources, while knowing that DHS must adapt and use the tools at its disposal to defeat these threats.

In particular, the privacy and FOIA professionals at DHS: (1) uphold the rights and principles of privacy and transparency in the third largest Department of the U.S. Government; (2) are an integral part of the DHS mission; and (3) are crucial to maintaining the public's trust. And if that's not enough, their hard work serves as the model for how other government agencies, and even entities outside the government, should approach their privacy and transparency responsibilities. Their accomplishments, including those demonstrated in this annual report, are a clear reminder that the DHS Privacy Office is the premier federal privacy office in the United States.

This report, as well as previous Annual Reports, can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

Please direct any inquiries about this report to the DHS Privacy Office at 202-343-1717 or privacy@dhs.gov.

Sincerely,

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

Pursuant to congressional notification requirements, this report is being provided to the following Members of Congress:

The Honorable Thomas R. Carper
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Coburn, M.D.
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Charles Grassley
Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Dianne Feinstein
Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Saxby Chambliss
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 Darrell Issa
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 Mike Rogers
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

Executive Summary

The Department of Homeland Security (DHS or Department) Privacy Office is the first statutorily created privacy office in any federal agency, as set forth in Section 222 of the *Homeland Security Act of 2002*, as amended.[1] The mission of the Privacy Office is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. The Privacy Office accomplishes its mission by focusing on the following core activities:

- Requiring compliance with federal privacy and disclosure laws and policies in all DHS programs, systems, and operations;
- Centralizing *Freedom of Information Act* and *Privacy Act* operations to provide policy and programmatic oversight, to support operational implementation within the DHS components, and to ensure the consistent handling of disclosure requests;
- Providing leadership and guidance to promote a culture of privacy and adherence to the Fair Information Practice Principles across the Department;
- Advancing privacy protections throughout the Federal Government through active participation in interagency fora;
- Conducting outreach to the Department's international partners to promote understanding of the U.S. privacy framework generally and the Department's role in protecting individual privacy; and,
- Ensuring transparency to the public through published materials, reports, formal notices, public workshops, and meetings.

This report, covering the period from July 1, 2013, through June 30, 2014, catalogues the Privacy Office's continued success in safeguarding individual privacy while supporting the DHS mission.

The Office's Fiscal Year 2012-2015 Strategic Plan includes five strategic goals:

- **Goal 1 (*Privacy and Disclosure Policy*)**: Foster a culture of privacy and transparency, and demonstrate leadership through policy and partnerships;
- **Goal 2 (*Advocacy*)**: Provide outreach, education, training, and reports in order to promote privacy and openness in homeland security;
- **Goal 3 (*Compliance*)**: Ensure that DHS complies with federal privacy and disclosure laws and policies and adheres to the DHS Fair Information Practice Principles;
- **Goal 4 (*Oversight*)**: Conduct robust oversight on embedded privacy protections and disclosures in all DHS activities; and
- **Goal 5 (*Workforce Excellence*)**: Develop and maintain the best privacy and disclosure professionals in the Federal Government.

[1] 6 U.S.C. § 142.

Key Privacy Office achievements during the reporting period, and the Office's associated strategic goals, are listed below. More details on each of these items, and additional achievements, can be found in the body of this report.

Goal 1: Privacy and Disclosure Policy

- Reaffirmed the Department's commitment to openness and transparency by issuing a new policy memorandum during the reporting period, *Freedom of Information Act and 2014 Sunshine Week*, highlighting some of the Department's accomplishments over the past year in furthering its openness and transparency initiatives.
- Provided leadership and privacy subject-matter expertise in DHS's ongoing evaluation of its information sharing with the Intelligence Community.
- Leveraged the expertise of the Data Privacy and Integrity Advisory Committee, which held two public meetings and issued one public report:
    - *Data Privacy and Integrity Advisory Committee Recommendations Paper 2013-01* , sets forth recommendations for DHS to consider when contemplating the use of live data in research, testing, or training, and for specific privacy protections DHS can consider when that live data includes personally identifiable information.

Goal 2: Advocacy

- Participated in interagency policy discussions on government-wide privacy issues related to federal use of Unmanned Aircraft Systems, the planned opening of the National Airspace System to private and commercial Unmanned Aircraft Systems, and the use of federal funds by state, local, tribal, and territorial governments to acquire Unmanned Aircraft Systems.
- Issued the first annual *Executive Order13636 Privacy and Civil Liberties Assessments Report;* the Executive Order requires that departments and agencies conduct assessments of the privacy and civil liberties impacts of activities undertaken to implement the Executive Order.
- Spearheaded a briefing of the DHS Data Framework Project for the White House's Big Data and Privacy Study, *Big Data: Seizing Opportunities, Preserving Value,* and contributed significantly to a chapter on the DHS Data Framework in the broader context of embedding privacy protections in government use of big data.
- Continued to support U.S. interagency talks with the European Commission to achieve a binding umbrella agreement with baseline standards for protecting personally identifiable information exchanged for law enforcement, criminal justice, and public security purposes.
- Acted as the Department lead on the new Privacy Task Force of the Five Country Conference, successfully obtaining agreement among all five countries to proactively share with one another their full Privacy Impact Assessments for all Five Country Conference projects.
- Continued to play a role in the federal interagency community through active participation and leadership roles in the Information Sharing and Access Interagency Policy Committee, the Federal Chief Information Officer Council Privacy Committee, and other interagency fora and initiatives.
- Issued congressionally-mandated public reports that document progress in implementing DHS privacy and Freedom of Information Act policy, and briefed Congress on privacy and *Freedom of Information Act*-related matters upon request.

Goal 3: Compliance

- Approved 56 new or updated Privacy Impact Assessments, and 19 System of Records Notices, resulting in a Department-wide Federal Information Security Management Act privacy score of 84 percent for required IT system Privacy Impact Assessments, and 94 percent for System of Records Notices. These scores are comparable to last year's scores of 82 percent for PIAs, and 95 percent for System of Records Notices.
- Published four Privacy Impact Assessments related to the DHS Data Framework, a scalable information technology program with built-in capabilities to support advanced data architecture and governance processes. This program will alleviate mission limitations associated with stove-piped Information Technology systems that are currently deployed across multiple operational Components in DHS.
- Reviewed 272 intelligence products and 259 Intelligence Information Reports. The Privacy Office is required by Departmental policy to review these products to ensure that the products adequately protect the privacy of individuals named in the products and reports.
- Deployed a web-based form on the external *Freedom of Information Act* website to facilitate the submission of electronic requests.

Goal 4: Oversight

- Completed a sixth Privacy Compliance Review for the Department's use of social media for situational awareness (*National Operations Center Publicly Available Media Monitoring and Situational Awareness Initiative*) and had two active Privacy Compliance Reviews in progress: a review of the Analytical Framework for Intelligence, and a review of the implementation of recommendations included in the 2012 Privacy Compliance Review for the EINSTEIN Program.
- Led a joint review with the European Commission of DHS compliance with the *Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security*, after which the European Commission published its mostly favorable findings.
- Promoted best practices in handling and mitigating privacy incidents by conducting site visits at DHS Components, presenting at two conferences for Federal Government personnel, and disseminating a customizable tip sheet *What You Need to Know About E-mailing Sensitive Personally Identifiable Information* to all Components.

Goal 5: Workforce Excellence

- Invested in training to promote greater understanding of *Freedom of Information Act* and *Privacy Act* requirements, as well as to broaden staff expertise in other mission areas, such as procurement, cybersecurity and information technology.
- Worked diligently to reduce expenses by eliminating onsite contractor support, expanding the use of in-house training, and reducing the use of office supplies. In addition, the Office utilized no-cost government facilities to host all of its internal and external training events, as well as to operate the public meetings of its federal advisory committee.

As this report demonstrates, the Privacy Office is an organization that both embodies and advances its vision of being a global leader in promoting and protecting privacy and transparency as fundamental to the American way of life.

Privacy Office

2014 Annual Report to Congress

Table of Contents

Legislative Language

This report has been prepared in accordance with the *Homeland Security Act of 2002* (Homeland Security Act), which includes the following requirement:

SEC. 222, as amended; 6 U.S.C. § 142 (Privacy Officer)

(a) Appointment and responsibilities-

The Secretary shall appoint a senior official in the Department, who shall report directly to the Secretary, to assume primary responsibility for privacy policy, including…

****

(6) preparing a report to Congress on an annual basis on activities of the Department that affect privacy, including complaints of privacy violations, implementation of the *Privacy Act of 1974* [5 U.S.C. § 552a], internal controls, and other matters.

Background

The DHS Privacy Office's (Privacy Office or Office) mission is to protect the privacy of all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. This report, covering the period from July 1, 2013 through June 30, 2014, catalogues the Office's continued success in safeguarding individual privacy while supporting the DHS mission.

Statutory Framework and the Fair Information Practice Principles

The *Homeland Security Act* charges the DHS Chief Privacy Officer with primary responsibility for ensuring that privacy considerations and protections are comprehensively integrated into all DHS programs, policies, and procedures. The *Privacy Act of 1974* (Privacy Act), the *Freedom of Information Act* (FOIA), and the *E-Government Act of 2002* all require DHS to be transparent in its operations and use of information relating to individuals. The Privacy Office centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight, and to support implementation across the Department. To facilitate this process, the Chief Privacy Officer is also the Chief FOIA Officer for the Department.

The Fair Information Practice Principles (FIPPs), presented in Figure 1, are the cornerstone of DHS's efforts to integrate privacy and transparency into all Department operations.[2]

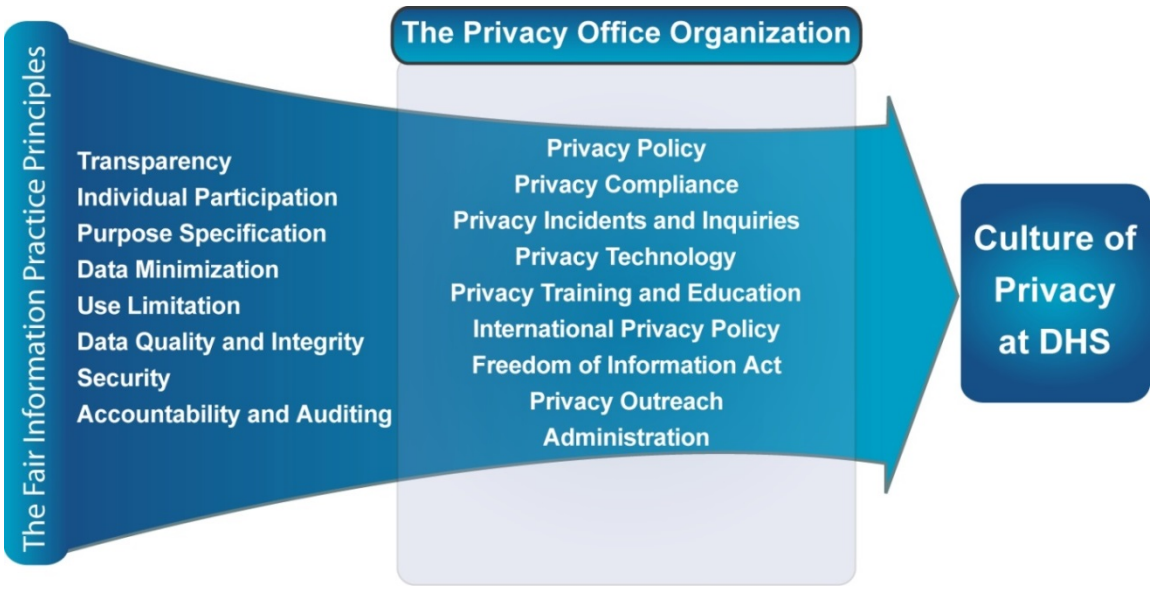


Figure 1: Privacy Office Implementation of the FIPPs

[2] The FIPPs are rooted in the *Privacy Act of 1974*, 5 U.S.C. § 552a, and memorialized in Privacy Policy Guidance Memorandum No. 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf, and in DHS Directive 047-01, *Privacy Policy and Compliance*, July 2011.

The Privacy Office incorporates these universally-recognized principles into privacy and disclosure policy and compliance processes throughout the Department. The Office also undertakes these statutory and policy-based responsibilities in collaboration with DHS Component privacy officers, privacy points of contact (PPOC),[3] DHS Component FOIA Officers, and program offices to ensure that all privacy and disclosure issues are afforded the appropriate level of review and expertise.

Office Structure

The work of the Privacy Office primarily supports three core DHS missions: preventing terrorism and enhancing security; securing and managing our borders; and safeguarding and securing cyberspace. Additionally, through training, outreach, and participation in program development and key Department agreements, the Office advances the 2014 Quadrennial Homeland Security Review goal of maturing and strengthening the homeland security enterprise.

The organizational structure of the Privacy Office is aligned with, and accountable for, its five strategic goals. Figure 2 depicts the organizational structure of the Office.

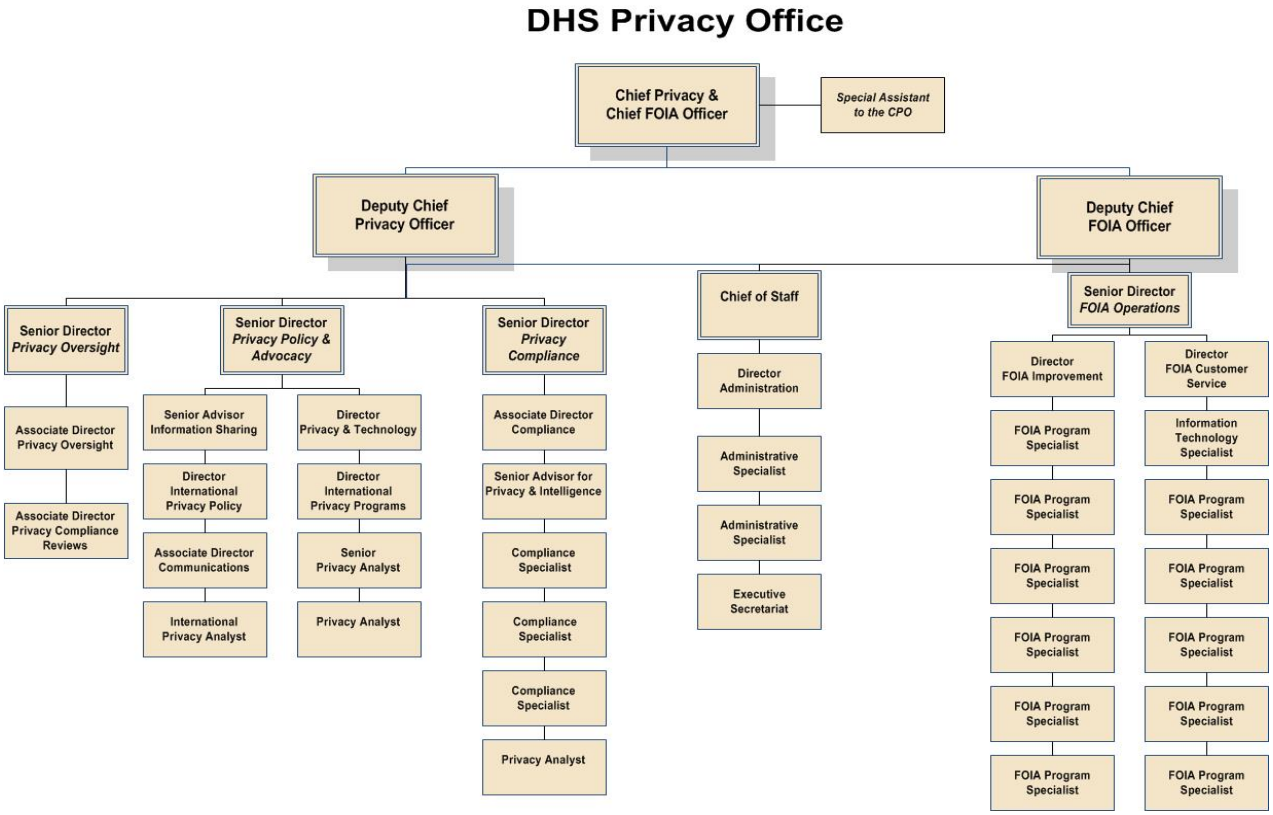


Figure 2: Privacy Office Organizational Chart

[3] PPOCs are assigned responsibility for privacy within their respective components, directorates, or programs, but they are not generally full-time privacy officers. Their privacy-related duties may be in addition to their primary responsibilities. Like Component Privacy Officers, PPOCs work closely with component program managers and the Privacy Office to manage privacy matters within DHS.

Privacy Policy and Advocacy Team (PPAT) bears primary responsibility for the development of DHS privacy policy, as well as providing subject matter expertise and support for policy development throughout the Department in areas that impact individual privacy, such as information sharing, enterprise data management, cybersecurity, international engagement, and intelligence products. PPAT is also responsible for supporting the privacy training, public outreach, and reporting functions of the Privacy Office.

Privacy Compliance Team oversees the privacy compliance activities for the Department, including supporting Component privacy officers, PPOCs, and DHS programs in completing Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), System of Records Notices (SORN), and other compliance documents. A brief description of the privacy compliance process can be found in Appendix C. The Privacy Compliance Team also manages the Privacy Office team that reviews intelligence products, and provides privacy support for DHS intelligence activities.

FOIA Team coordinates Department-level compliance with FOIA by developing Department-wide policy needed to implement important FOIA initiatives, such as the sweeping changes set forth in the President's FOIA Memorandum and the Attorney General's FOIA Guidelines of 2009. Additionally, the FOIA Team coordinates and oversees Component FOIA operations, provides FOIA training, and prepares required annual reports of the Department's FOIA performance. The FOIA Team also processes initial FOIA and Privacy Act requests on behalf of the Office of the Secretary (including the Military Advisor's Office and the Office of Intergovernmental Affairs (IGA)), and nine DHS Components (DHS FOIA Office Components).

Privacy Oversight Team is dedicated to implementing accountability and continuous improvement of DHS privacy processes and programs. Its responsibilities include conducting Privacy Compliance Reviews (PCR) and investigations, managing the Department's privacy incident response efforts, and overseeing the Department's handling of privacy complaints.

Privacy Administrative Coordination Team (PACT) focuses on recruiting and maintaining a superior workforce of talented subject-matter experts and ensuring the efficiency of office operations. In addition to providing administrative support for all Privacy Office functions, PACT also manages resources, planning, official correspondence, workforce policy, staff development, resilience, facilities, and other infrastructure.

I. Privacy and Disclosure Policy

The Office's Fiscal Year (FY) 2012-2015 Strategic Plan includes five strategic goals:

Privacy Office Strategic Goal 1 (Policy)*: Foster a culture of privacy and transparency and demonstrate leadership through policy and partnerships.*

This section highlights the Office's development and support of new policy initiatives to further privacy and transparency at DHS during the reporting period.

DHS Mobile Application Policy Development

As the public's use of mobile technology has become the norm, DHS has begun to develop and deploy mobile applications (apps) for public use. Apps are beneficial because they allow users to receive information, such as news updates or other alerts, from their mobile devices while on the go. The mobility of devices also allows users to provide the timeliest information even when they do not have immediate access to a computer.

While mobile apps offer numerous benefits they can pose potential privacy concerns because of the unique but commonly used capabilities of mobile technology, such as location services and the use of unique device identifiers. As a result of the relationship between mobile devices and

Personally Identifiable Information (PII) or other sensitive information, the Privacy Office has made it a priority to ensure that appropriate privacy protections are incorporated into mobile apps developed by DHS by initiating a process a process to create a mobile app privacy policy and compliance documentation. Although the FIPPs and other privacy policies provide a framework to ensure privacy protection in all Department activities, a policy that is specific to mobile apps will help ensure that the overall DHS privacy framework is applied consistently to address mobile apps' unique privacy impacts, and will promote transparency about DHS's mobile app privacy practices.

To develop a well-informed policy, the Privacy Office conducted a comprehensive review of Components' existing mobile applications and compliance documentation to identify their existing mobile app privacy practices. The Office also researched the various types of mobile apps, industry and government mobile app privacy practices, and advocacy groups' recommended practices, to identify potential mobile app policy requirements for DHS. The Privacy Office will consult with various Components for their feedback on a draft policy. By developing a mobile app policy, DHS can embrace the benefits of mobile applications while protecting privacy and promoting transparency.

Information Sharing Policy Leadership

During the reporting period, the Privacy Office collaborated with Component privacy offices, the DHS Office of Intelligence and Analysis (I&A),[4] Office for Civil Rights and Civil Liberties (CRCL), the Office of Policy (PLCY), DHS Component data stewards, and external information sharing partners to ensure that the Department executes its information sharing programs in a privacy-protective manner. Through these collaborative relationships, the Office:

- Provided leadership and privacy subject-matter expertise in DHS's ongoing evaluation of its information sharing with the Intelligence Community (IC).
  - After the U.S. Attorney General approved new *Guidelines for Access, Retention, Use, and Dissemination by the National Counterterrorism Center and other Agencies of Information in Data sets Containing Non-Terrorism Information*,[5] the Privacy Office participated in the development of new Information Sharing Access Agreements (ISAA) with the National Counterterrorism Center[6] (NCTC). These ISAAs include new privacy protections related to transparency, oversight, and redress.
  - The Privacy Office continued to participate in quarterly reviews of NCTC's use of DHS data, including its application of baseline safeguards.[7]

[4] The DHS Undersecretary for I&A is the chair of the DHS Information Sharing and Safeguarding Governance Board and the Department's designated Information Sharing Executive.
[5] The Guidelines were approved in March 2012 and are available at: http://fas.org/sgp/othergov/intel/nctc_guidelines.pdf
[6] NCTC is the primary organization in the United States Government for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism possessed or acquired by the United States Government. The Privacy Office has maintained a leadership role in DHS's engagement with NCTC for the past several reporting periods.
[7] More information on NCTC's data stewardship is available through its Transparency Initiative at http://www.nctc.gov/transparency.html.

- In May 2014, the Department assigned its first on-site oversight representative to NCTC from the DHS Privacy Office. This senior-level assignee provides privacy policy oversight and will draft an overarching PIA with NCTC to provide more transparency regarding DHS's information sharing relationship with NCTC.
- Through the Information Sharing and Access Interagency Policy Committee's Mission Information Sharing Restricted Subcommittee, the Privacy Office also participated in discussions with the Office of the Director of National Intelligence (ODNI) and interagency partners to discuss the privacy implications of sharing non-Title 50 information[8] with the IC. Most DHS information is not collected under intelligence authorities, and thus carries legal and policy considerations that may be different than the legal and policy considerations associated with intelligence information.

- Maintained an active leadership role in DHS's internal information sharing and management governance processes.
  - The Privacy Office remained an active participant in the DHS Information Sharing and Safeguarding Governance Board (ISSGB) and the DHS Information Sharing Coordinating Council (ISCC).
  - Through the ISCC and ISSGB, the Privacy Office supported the development of the DHS Information Sharing and Safeguarding Strategy and the DHS Information Sharing and Safeguarding Strategy Implementation Plan. The Implementation Plan includes "Priority Objective 13: Privacy, Civil Rights, and Civil Liberties Compliance Processes," which promotes enhanced privacy oversight of DHS's ISAAs and is co-led by the Privacy Office and CRCL.
  - As part of the ISCC, the Privacy Office also participated in the Data Access Request Process Working Group, which seeks to memorialize and automate DHS's internal clearance processes for ISAAs and ensure that the Office of the General Counsel (OGC), CRCL, and the Privacy Office are able to review DHS ISAAs with external entities.

  - As part of the ISSGB Law Enforcement Shared Mission Community (LESMC), a Privacy Office speaker addressed over two hundred law enforcement officers from around the country at the Law Enforcement Information Sharing Initiative Annual Roundtable. By attending monthly LESMC meetings, the Privacy Office gains insight into the information sharing needs of DHS law enforcement operators and is able to engage in collaborative dialog on ways to address those needs in a privacy-consistent manner.
  - As part of the DHS Records Working Group, the Privacy Office contributed to draft DHS policies on sharing information related to asylum seekers, asylees, and refugees, and reviewed the protections in ISAAs for information related to certain special protected classes of aliens, as required by 8 U.S.C. § 1367.

[8] Title 50 of the United States Code.

- As a member of the DHS Office of Biometric Identity Management (OBIM), formerly known as United States Visitor and Immigrant Status Indicator Technology (US-VISIT),[9] Executive Steering Committee, the Privacy Office continued to work with OBIM to develop new processes for coordination with data owners to improve privacy and information sharing policy compliance.
- The Chief Privacy Officer serves as a member of the Homeland Security Information Network[10] (HSIN) Executive Steering Committee, and partners with the DHS Office of the Chief Information Officer (OCIO) and the operational Components across the Department to integrate privacy compliance into the architecture of the next generation of HSIN.
- The Chief Privacy Officer serves as a member of the Department's Identity, Credentialing and Access Management (ICAM) Executive Steering Committee. The Office communicated closely with OCIO's strategists and developers as they continued to develop the Department's consolidation and advances in ICAM services. Through ICAM's planning and technologies, OCIO plans to create a trusted identity system of integrated capabilities and supporting infrastructure to enable individuals and computer systems to verify identities through an automated trusted authentication authority at the enterprise level.
- During this reporting period, the Deputy Chief FOIA Officer participated in the Executive Steering Committee for Information Governance. The Deputy Chief FOIA Officer provided advice on strategic improvement opportunities, including the potential increased use of technology to enhance the Department's overall FOIA operations.
- During this reporting period, the Deputy Chief Privacy Officer served on the DHS International Governance Board (IGB), chaired by the Assistant Secretary for International Affairs. The IGB created a Working Group on How to Strengthen the International Affairs Enterprise in Support of DHS Missions. Privacy Office staff provided input on an evaluation of the current international affairs coordination function, and made contributions to a draft strategic plan to encourage effective coordination of new international information sharing initiatives that are consistent with privacy law and policy.

- Provided information sharing policy leadership in DHS's internal information sharing and aggregation activities.
  - Through the DHS Common Vetting Task Force, the Privacy Office collaborated on the development of the DHS Data Framework, a scalable information technology program that will support advanced data capabilities under formal governance processes.[11] At this

[9] In March 2013, the *Consolidated and Further Continuing Appropriations Act,2013* transferred the legacy US-VISIT overstay analysis mission to ICE and entry/exit policy and operations to CBP. The Act also transferred the biometric identity management functions to OBIM, a newly created office within NPPD.

[10] The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive But Unclassified information. Federal, state, local, tribal, territorial, international and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and in general, share the information they need to do their jobs.

[11] *See* "Privacy Impact Assessment for the DHS Data Framework," November 6, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf.

time, the Data Framework is composed of three pilot initiatives: the Cerberus Pilot,[12] the Common Entity Index (CEI) Prototype,[13] and the Neptune Pilot.[14] These initiatives use data tags to apply policy-based rules to determine which users can access which data for what purpose, so DHS can share its information internally while ensuring that robust policy and technical controls are in place to protect privacy.
  - The Privacy Office hosted public briefings on the Data Framework initiatives during public meetings of the Data Privacy and Integrity Advisory Committee[15] (DPIAC), the Department's privacy advisory committee established by the Secretary under the *Federal Advisory Committee Act*[16] (FACA), providing an opportunity for members of the public to ask questions about the initiatives. The Chief Privacy Officer also tasked the DPIAC with developing recommendations on additional audit and oversight capabilities for the Data Framework initiatives. See page 16 for more information on the DPIAC's work.

- Reviewed DHS ISAAs for FIPPs-based privacy protections.
  - In coordination with the ISCC, the Privacy Office participated in reviews of ISAAs to ensure compliance with DHS privacy policies and ISCC guidance. These reviews included ISAAs with international, federal, state, local, territorial, and tribal partners. The Privacy Office reviews ISAAs for their compatibility with applicable privacy documentation, and for the FIPPs - based privacy protections, such as limits on data retention, use, and dissemination; avenues for access and redress; and provisions for data security and integrity, accountability, and auditing.

Fusion Center Support

In 2007, the Implementing Recommendations of the 9/11 Commission Act (9/11 Commission Act) established the DHS State, Local, and Regional Fusion Center Initiative, thereby codifying an existing relationship between DHS and a national network of fusion centers. The DHS Privacy Office has exercised leadership in establishing and growing a robust privacy protection framework within the fusion center program, both at the national and state levels.

Privacy Office staff provided the following training this year in collaboration with CRCL:

1. Privacy training for intelligence professionals selected for assignment to fusion centers, as required under section 511 of the 9/l1 Commission Act. This course focuses on the privacy analysis of intelligence investigative reports and analytic products. Twelve DHS intelligence officers were trained in three sessions.

[12] *See* "Privacy Impact Assessment for the Cerberus Pilot," November 22, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-cerberus-nov2013.pdf.
[13] *See* "Privacy Impact Assessment for the Common Entity Index Prototype (CEI Prototype)," September 26, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-cei-pilot-_09262013.pdf.
[14] *See* "Privacy Impact Assessment for the Neptune Pilot," September 25, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-neptune-09252013.pdf.
[15] See the DHS Privacy Office website for more information about the advisory committee, its briefings on the Data Framework, and the recent tasking.
[16] 5 U.S.C. Appendix

2. Train-the-Trainer session to provide newly-appointed fusion center privacy officers with guidance on how to establish a robust privacy program, as well as instruction on how to train their staff to safeguard privacy using the FIPPs. The privacy officers from 12 fusion centers were trained in one session.

Disclosure and Transparency Policy Initiatives

The Privacy Office reaffirmed the Department's commitment to openness and transparency by issuing a new policy memorandum during the reporting period:

Freedom of Information Act and 2014 Sunshine Week, issued in March 2014, highlighted some of the Department's accomplishments over the past year in furthering its openness and transparency initiatives. The Memorandum also asked FOIA Officers to remind all staff about the U.S. Attorney General's call to action in his FOIA guidelines, issued March 19, 2009,[17] that "FOIA is everyone's responsibility."

Data Privacy and Integrity Advisory Committee

The DPIAC[18] provides advice to the Department at the request of the Secretary of Homeland Security and the Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to PII, data integrity, and other privacy-related matters.[19]

The DPIAC met in public session twice during the reporting year:

- On September 12, 2013, DHS briefed the Committee on unmanned aircraft systems, on *Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity*, and the Department of Homeland Security Information Sharing Environment (ISE). The Committee then presented its research findings regarding privacy considerations in the Department's use of live data for training purposes, for testing new or updated systems, and for research. The report was finalized and posted on the DPIAC website:
    - *DPIAC Recommendations Paper 2013-01, September 12, 2013, (PDF 654 KB, 19 pages)*, sets forth recommendations for DHS to consider when contemplating the use of live data in research, testing, or training, and for specific privacy protections DHS can consider when that live data includes PII.

[17] The Attorney General's Memorandum of March 19, 2009, is available at http://www.usdoj.gov/ag/foia-memo-march2009.pdf.

[18] All DPIAC reports, along with membership and meeting information, are posted on the Privacy Office website, www.dhs.gov/privacy.

[19] The Committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. § 451 and operates in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App 2. DPIAC members serve as Special Government Employees and represent a balance of interests on privacy matters from academia, the private sector (including for-profit and not-for-profit organizations), state government, and the privacy advocacy community. The DPIAC provides advice on matters assigned to it by the Chief Privacy Officer and conducts its deliberations in public meetings.

- On January 30, 2014, the Committee met both online and in Washington, D.C. The Privacy Office Senior Director of Compliance led a discussion on DHS federated information sharing policy and technology practices, or "big data," and the Cerberus, Neptune, and the CEI Prototype pilots (see greater detail under Information Sharing Policy Leadership above). The Chief Privacy Officer tasked the Committee with researching ways to improve transparency and oversight in the Department's Data Framework.

On May 28, 2014, the Secretary of Homeland Security appointed or reappointed nine DPIAC members.

II. Advocacy

The Office's FY 2012-2015 Strategic Plan includes five strategic goals:

Privacy Office Strategic Goal 2 (Advocacy): *Provide outreach, education, training, and reports in order to promote privacy and openness in homeland security.*

This section highlights the ways in which Privacy Office staff partners with DHS operational personnel and their counterparts at other federal agencies to shape programs and embed privacy protections and proactive disclosure policies into the activities, dialogue, and products of the entire homeland security enterprise.

Interagency Leadership

Unmanned Aircraft Systems (UAS)

Privacy Office staff participate in interagency policy committee and sub-committee discussions on government-wide privacy issues related to federal use of UAS, the planned opening of the National Airspace System to private and commercial UAS, and the use of federal funds by state, local, tribal, and territorial governments to acquire UAS. The DHS Privacy Office offers unique perspectives, as DHS is the only agency to research, draft, and publish Privacy Impact Assessments on UAS. In addition, Privacy Office staff are able to bring knowledge gained

through the DHS Privacy, Civil Rights, and Civil Liberties Working Group on UAS (mentioned below) to a larger interagency community for consideration in policy development.

The Privacy Office is also working to achieve the highest level of transparency in its work on UAS. During the reporting period, Privacy Office senior staff briefed the Senate Judiciary Committee Majority Staff, the Congressional Unmanned Aircraft Systems Caucus, the Homeland Security & Governmental Affairs Committee Staff, and the Senate Appropriations Committee Staff on UAS privacy issues at DHS. In addition, the Chief Privacy Officer and the Deputy Chief Privacy Officer discussed UAS issues in their other briefings with Senate and House committees. Senior staff explained the Aircraft Systems PIA to the DPIAC shortly before it was published, held two sessions with advocacy groups, briefed Government Accountability Staff on two occasions, and met with the Congressional Research Service Staff once. Many of these activities included United States Customs and Border Protection (CBP) and CRCL staff so that those in attendance could receive a comprehensive briefing on UAS issues.

DHS Privacy, Civil Rights, and Civil Liberties Working Group on UAS[20]

The Privacy Office co-chairs this Working Group, which was created to provide a forum for all Components whose work relates in some way to UAS activities to discuss items of common interest, and to coordinate guidance on privacy, civil rights, and civil liberties issues. The Working Group compiled a best practices document that reflects the lessons learned through the Department's operation of UAS. The best practices principles enumerated in the document may be used by any Component whose future plans include funding or deploying UAS. These best practices may also inform state and local law enforcement agencies of issues to consider when establishing a UAS program. The best practices document should be published later this year.

Cybersecurity of Critical Infrastructure

On February 12, 2013, President Obama issued two important directives to federal departments and agencies on strengthening the Nation's critical infrastructure: *EO 13636*, and *Presidential Policy Directive (PPD)-21*, *Critical Infrastructure Security and Resilience.*[21] Together, these documents recognize the increased role of cybersecurity in securing physical assets, and require a comprehensive public and private sector effort to ensure the security and resilience of cyber

[20] Memorandum For The Secretary from Tamara J. Kessler, Acting Officer for Civil Rights and Civil Liberties and Jonathan R. Cantor, Acting Chief Privacy Officer, "Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department's Use and Support of Unmanned Aerial Systems (UAS)" September 14, 2002, https://www.dhs.gov/sites/default/files/publications/foia/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-s1-information-memorandum-09142012.pdf.

[21] The Executive Order is available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf. Presidential Policy Directive 21 is available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

and physical critical infrastructure in a manner that protects both privacy and civil liberties. EO 13636 requires that departments and agencies conduct assessments of the privacy and civil liberties impacts of activities they undertake to implement EO 13636. At DHS, this responsibility falls to both the Privacy Office and CRCL.

Section Five of EO 13636 also requires that senior agency officials for privacy and civil liberties publish their assessments annually in a report compiled by the Privacy Office and CRCL. The Chief Privacy Officer and Officer for Civil Rights and Civil Liberties issued the first annual *EO 13636 Privacy and Civil Liberties Assessments Report* in April 2014. The Report includes the Privacy Office's and CRCL's assessments of DHS activities supporting enhanced threat information sharing with the private sector. It also includes submissions and assessments conducted independently by the Department of the Treasury and the Departments of 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.[22]

Together with NPPD and I&A privacy officers, whose components have primary responsibility for implementing EO 13636, the Privacy Office has been deeply involved in the development of the programs required by EO 13636, thereby ensuring that privacy protections are implemented. In conducting its assessments, the Privacy Office used the FIPPs framework that it uses to evaluate the privacy impact of any DHS system or initiative, as required by DHS Directive 047-01, *Privacy Policy and Compliance* (July 2011).

The Privacy Office will continue to oversee the Department's cybersecurity initiatives as these programs and activities mature and evolve, and, together with CRCL, will conduct additional assessments as needed and include them in future annual EO 13636 Reports.

Other Interagency Initiatives

During the reporting period, the Office continued its active engagement and leadership roles in key interagency fora and initiatives.

White House Big Data and Privacy Study. The Chief Privacy Officer spearheaded a briefing of the DHS Data Framework Project for the White House's Big Data and Privacy Study, *Big Data: Seizing Opportunities, Preserving Value*, and the Privacy Office made significant contributions to a chapter on the DHS Data Framework in the broader context of embedding privacy protections in government use of big data.

Information Sharing and Access Interagency Policy Committee (ISA-IPC*).* The ISA-IPC develops strategic, cross-cutting approaches to address information sharing and safeguarding policy matters related to national security. The ISA-IPC is comprised of federal ISE mission partners, and is supported by subcommittees and working groups with federal, state, local, and tribal participation. The ISA-IPC is co-chaired by the White House National Security Council staff and the Program Manager for the ISE at the ODNI.

[22] The Report is available on the DHS Cybersecurity and Privacy web page at: http://www.dhs.gov/publication/executive-order-13636-privacy-and-civil-liberties-assessment-report-2014.

Through participation in the ISA-IPC, the Privacy Office maintains its leadership role in advancing privacy protections through the development of sound information sharing policies, both within DHS and across the Federal Government. The Privacy Office also supports ISA-IPC efforts to implement the 2013 National Strategy for Information Sharing and Safeguarding,[23] which outlines a path towards increased consistency in the application of mission-appropriate privacy, civil rights, and civil liberties protections across the ISE by building safeguards into the development and implementation of information sharing programs and activities.

Privacy and Civil Liberties Subcommittee. The Chief Privacy Officer is a designated co-chair and member of the ISA-IPC Privacy and Civil Liberties (P/CL) Subcommittee, an interagency governance body focused on the enhancement of privacy, civil rights, and civil liberties protections in information sharing activities to support national and homeland security. The P/CL Subcommittee facilitates the adoption and implementation of policies consistent with the ISE Privacy Guidelines[24] by organizations participating in the ISE.

Privacy Office staff also support Subcommittee working groups that focus on developing tools to help ISE mission partners consistently apply privacy, civil rights, and civil liberties protection requirements. During the reporting period, this support included assistance in standing up a new Training Working Group and developing a Framework of Considerations Reference Guide and checklist worksheet to support the National Strategy for Information Sharing and Safeguarding's Priority Objective for streamlining the information sharing and access agreement development process.

National Science and Technology Council (NSTC),[25] Subcommittee on Privacy and Internet Policy, International Working Group. Privacy Office staff regularly contribute to the work of the NSTC Subcommittee on Privacy and Internet Policy International Working Group. The Working Group serves as an interagency forum for discussion on emerging international privacy issues, and is a valuable resource for staying apprised of international privacy engagement undertaken by the Federal Government.

The Federal CIO Council[26] Privacy Committee (Privacy Committee). The Deputy Chief Privacy Officer continued to serve as co-chair of the Federal CIO Council Privacy Committee, the principal interagency forum for improving federal agency privacy practices. The Privacy Committee serves as the interagency coordination group for Senior Agency Officials for Privacy (SAOP) and Chief Privacy Officers in the Federal Government. It provides a consensus-based forum for the development of privacy policy and protections throughout the Federal Government by promoting adherence to the letter and spirit of federal privacy law and policy.

[23] http://www.dhs.gov/sites/default/files/publications/12-4466-dhs-information-sharing-and-safeguarding-strategy-01-30-13--fina%20%20%20.pdf
[24] http://ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf
[25] The NSTC was established by EO 12881 on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise.
[26] The Federal CIO Council was first established by EO 13011 in 1996 and later codified by Congress in the E-Government Act of 2002. The CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. *See* the CIO Council Privacy Committee website at https://cio.gov/about/groups/privacy-cop/.

Privacy Office and Component privacy office staff supported the following subcommittees and Privacy Committee initiatives:

- **Best Practices Subcommittee** – Last year this Subcommittee collaborated with the National Institute for Standards and Technology (NIST) to incorporate a comprehensive set of privacy controls (Appendix J) into NIST Special Publication 800-53, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations (Rev. 4) (SP 800-53).* This year the Subcommittee has formed a Metrics Working Group to develop key metrics to ensure compliance with implementation of Appendix J controls.
- **Identity Management (IdM) Subcommittee** – This Subcommittee has been focused on reviewing the updated FICAM Trust Framework Solutions (TFS) Program (from 2009). It also provided feedback regarding the privacy aspects of the Federal Cloud Credential Exchange (FCCX) Pilot, an identity broker shared service to support the implementation of the TFS program. The Pilot will help facilitate the FICAM Program – with fewer privacy risks.
- **Development and Education Subcommittee** – This Subcommittee is busy planning the 2014 Privacy Summit, a training event to encourage collaboration between executive branch agency privacy offices and their key business partners, including CIO and procurement staff. The Subcommittee also sponsored a training session for agency management officials to share Appendix J implementation issues, including lessons learned and challenges.
- **Innovation and Emerging Technology Subcommittee** – This Subcommittee has spent the past year developing white papers on big data, data loss prevention tools, and biometrics. It also updated its white paper on privacy best practices for social media use, published by the CIO Council in July 2013.

International Engagement and Outreach

DHS works closely with international partners, including foreign governments and major multilateral organizations, to strengthen the security of the networks of global trade and travel upon which the Nation's economy and communities rely. When those engagements involve programs to share personal information or establish privacy best practices, the Privacy Office provides expertise to ensure that the DHS position is consistent with U.S. law and DHS privacy policy. By advancing Department privacy compliance practices to international partners and promoting the FIPPs, the Office builds the confidence necessary for cross-border information sharing and cooperation.

U.S. - Canada Beyond the Border Action Plan. Since the issuance of the *Beyond the Border* Declaration[27] by President Obama and Canadian Prime Minister Harper in February 2011, and the release of the *Beyond the Border Action Plan*,[28] the Privacy Office has focused on embedding and implementing the Joint Statement of Privacy Principles (Beyond the Border Privacy Principles) in Beyond the Border (BTB) initiatives. Implementation is achieved through:

- **Training** – The Privacy Office has developed flexible training materials on the BTB Privacy Principles. As implementation begins on any new BTB project, the Office is prepared to consult with project leads and deliver tailored training. The Office continues to assess the need for any follow-up training for ongoing projects.
- **Document Review** – Per DHS policy and in accordance with the BTB Privacy Principles, the Privacy Office reviews all BTB ISAAs and works with Component privacy offices to develop or update privacy compliance documentation such as PIAs and SORNs.
- **Consultation** – The Privacy Office provided advice and assistance with drafting and negotiating agreements for BTB projects, including:
  - **Immigration Information Sharing Agreement** – Upon finalization of the *U.S. - Canada Immigration Information Sharing Agreement*,[29] signed in December 2012, the Office participated in completing implementation documentation for biographic information sharing under the Agreement.
  - Biographic sharing under the Agreement began in January 2014, and the Privacy Office has assisted in monitoring progress and reviewing quality assurance assessments to ensure that the privacy protections that were incorporated into the Agreement are followed. Privacy compliance documentation for biographic sharing was updated before sharing began.
  - The Privacy Office continues to consult in efforts to develop implementing documentation for biometric sharing under the Immigration Information Sharing Agreement. The Office will ensure appropriate privacy provisions are incorporated in accordance with U.S. law, DHS policy, and the BTB Privacy Principles. Privacy compliance documentation will be issued or updated as necessary.
- **Entry/Exit Program** – The Office assisted in the continuing implementation of the BTB Entry/Exit Program, which establishes coordinated entry and exit systems at the common land border to exchange biographical information on the entry of travelers. Under this program, the record of an entry into one country establishes a record of exit from the other, ultimately supporting each country in its immigration and law enforcement missions while facilitating legitimate cross-border travel. The Office is providing ongoing consultation and

[27] http://www.whitehouse.gov/the-press-office/2011/02/04/declaration-president-obama-and-prime-minister-harper-canada-beyond-bord.
[28] http://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf.
[29] The U.S.-Canada Immigration Information Sharing Agreement provides for biographic and biometric information to be exchanged on third-country nationals to assist in the administration and enforcement of U.S. and Canadian immigration laws, respectively.

review of implementing documentation for Phase III. Privacy compliance documentation, such as PIAs and SORNs, will be developed or updated as necessary for Phase III.[30]

In addition to the training, document review, and consultation services that the Office provides, in June 2014, the Chief Privacy Officer travelled to Ottawa, Canada to discuss progress on BTB projects and implementation of the BTB Privacy Principles with Canadian government officials and the U.S. Ambassador to Canada.

U.S. - EU Data Privacy and Protection Agreement. The Chief Privacy Officer and Privacy Office staff continued to support the U.S. interagency talks with the European Commission to achieve a binding umbrella agreement with baseline standards for protecting PII exchanged for law enforcement, criminal justice, and public security purposes. The Chief Privacy Officer provided subject matter expertise on how the U.S. could satisfy the EU's requirement that its citizens enjoy the right of judicial redress for wrongful disclosure or refusal to correct inaccurate information as U.S. Persons – U.S. citizens and Lawful Permanent Residents – enjoy under the Privacy Act. In addition, the Chief Privacy Officer actively participated as a member of the U.S. delegation negotiating the language to the agreement with the European Union.

The Five Country Conference (FCC). Privacy Office staff continued to support the Policy-led engagement with the governments of Australia, Canada, New Zealand, and the United Kingdom under the Five Country Conference, to improve information sharing in immigration and border security. During the reporting period, the FCC created a new Privacy Task Force to assess the privacy and information sharing laws and policies of the member countries and how they may impact information sharing goals. Privacy Office staff act as the lead for the Department on the Privacy Task Force, and were successful in obtaining agreement among all five countries to proactively share with one another their full PIAs for all FCC projects. The Office continued to work on negotiation of agreements with FCC partner countries on the sharing of visa, immigration, and nationality information, similar to the one which was signed with the United Kingdom in April 2013.

Trans-Pacific Partnership and International Services Agreement. The DHS Office of Trade Policy leads DHS's coordination on these multilateral trade negotiations. Privacy Office staff provided guidance on DHS positions regarding government collection and handling of personal information.

A complete list of Privacy Office engagement with international visitors can be found in Appendix G.

[30] For Phase I, DHS published the Western Hemisphere Travel Initiative (WHTI): Beyond the Border Entry/Exit Program Phase I PIA, available at: http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/privacy_pia_cbp_whtibtb_sept2012.pdf. For Phase II, DHS published the Beyond the Border Entry/Exit Program Phase II PIA, available at: http://www.dhs.gov/publication/dhscbppia-004g-beyond-border-entryexit-program-phase-ii.

Privacy & FOIA Training and Awareness

Outreach

Throughout this reporting period, the Privacy Office developed, sponsored, and participated in events aimed at educating and engaging the federal workforce, the advocacy community, and the public on privacy-related topics, including:

Figure 1: Privacy Man Mascot

- **Annual Privacy Workshop**: In June 2014, 196 personnel from 42 federal agencies attended the Privacy Office's Annual Privacy Workshop. This one-day workshop provides in-depth training on DHS's privacy compliance processes and best practices, as well as on other important privacy topics.
- **Privacy advocate meetings**: The Chief Privacy Officer hosts periodic informational meetings with members of the privacy advocacy community, and keeps them informed of key privacy-related policies, reports, and activities by e-mail throughout the year.
- **Speaking engagements**: Privacy Office staff spoke at many conferences and events during this reporting period. See Appendix E for a detailed list.
- **Chief Privacy Officer's blog:** The Chief Privacy Officer publishes blog posts to inform the public of key accomplishments. In May 2014, a blog was posted to announce the celebration the Privacy Office's tenth anniversary.

Staff Training

The Privacy Office develops and delivers a variety of privacy and transparency-related training to DHS personnel.

- **New employee training**:
  - The Privacy Office provides privacy and FOIA training as part of the Department's bi-weekly orientation session for all new Headquarters employees.
  - The Office also provides monthly privacy training as part of the two-day course, *DHS 101*.
- **Annual online privacy awareness refresher training**: "Privacy at DHS: Protecting Personal Information" is mandatory for all DHS personnel when they join the Department, and annually thereafter.
- **Privacy training for Office of the Chief Human Capital Officer (CHCO) staff**: The Privacy Office trained all Headquarters CHCO staff on best practices for safeguarding PII.
- **Reports Officer certification course**: Office staff teaches the privacy module of this certification program for officers who prepare intelligence reports.
- **DHS Security Specialist course**: The Office provides privacy training each month to participants of this week-long training program sponsored by the Office of the Chief Security Officer.
- **DHS 201 international attaché training:** This week-long course is designed to prepare DHS employees who serve as DHS attachés at U.S. embassies worldwide by providing them with basic information on each Component's international activities. The Privacy Office provides an international privacy policy module to raise awareness among new attachés about U.S. privacy law and DHS privacy policy and practice.

- **FOIA training for the Components**: During the reporting period, the Privacy Office provided training on its commercial off-the shelf web application solution and an overview of processing Freedom of Information Act requests. The Privacy Office conducted 22 full-day training sessions for the Federal Emergency Management Agency (FEMA), Transportation Security Administration (TSA), United States Immigration and Customs Enforcement (ICE), Office of Inspector General (OIG), Science and Technology Directorate (S&T), NPPD, and I&A, plus 10 additional brief training sessions Privacy Office staff.
- **FOIA Annual Report training and best practices**: In September 2013, the Privacy Office provided a one-day FY 2013 Annual Report Refresher Training to the Component FOIA staff that included the reporting requirements and best practices for responding to FOIA requests.

Reporting

The Office issues congressionally-mandated public reports that document progress in implementing DHS privacy and FOIA policy, including this report. During the reporting period, the Office issued the following reports, which can be found on our website at www.dhs.gov/privacy.

- **Quarterly Reports under Section 803 of the 9/11 Commission Act**: The Office issued four quarterly reports to Congress as required by Section 803 of the 9/11 Commission Act. These reports include: (1) the number and types of privacy reviews undertaken by the Chief Privacy Officer; (2) the type of advice provided and the response given to such advice; (3) the number and nature of privacy complaints received by the Department; and (4) a summary of the disposition of such complaints and the reviews and inquiries conducted. In addition, the Office provided statistics on privacy training and awareness activities conducted by the Department to help prevent privacy incidents.

- ***Annual FOIA Report to the Attorney General of the United States***: This report provides a summary of Component-specific data on the number of FOIA requests received by the Department, the disposition of such requests, reasons for denial, appeals, response times, pending requests, processing costs, fees collected, and other statutorily required information.

- ***Chief Freedom of Information Act Officer Report to the Attorney General of the United States***: 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 requests, increases proactive disclosures, fully utilizes technology, reduces backlogs, and improves response times.

- ***DHS Data Mining Report to Congress***: This report describes DHS activities already deployed or under development that fall within the *Federal Agency Data Mining Reporting Act of 2007*[31] definition of data mining.

The Chief Privacy Officer and Privacy Office staff provided briefings to members of Congress on privacy and FOIA-related matters upon request. See Appendix F for a complete list of briefings during this reporting period.

[31] 42 U.S.C. § 2000ee-3.

III. Compliance

The Office's FY 2012-2015 Strategic Plan includes five strategic goals:

Privacy Office Strategic Goal 3 (Compliance): *Ensure that DHS complies with federal privacy and disclosure laws and policies and adheres to the DHS Fair Information Practice Principles (FIPPs).*

During the reporting period, the Privacy Office continued its efforts to ensure that both privacy and FOIA compliance are integrated into all DHS operations.

Privacy Compliance

The Privacy Office ensures privacy protections are built into Department systems, initiatives, and programs as they are developed and modified. The Office integrates privacy into Department operations by supervising and approving all DHS privacy compliance documentation, including PTAs, PIAs, and SORNs. The DHS PTA, PIA, and SORN templates and guidance are recognized government-wide as best practices and leveraged by other government agencies.

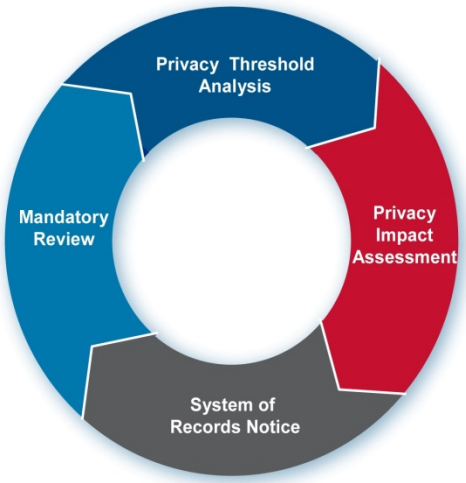


Figure 3: Privacy Office Compliance Process

The Privacy Office uses PIAs to establish guidelines based on the FIPPs for Department programs, systems, initiatives, and rulemakings. The Office is responsible for ensuring that the Department meets statutory requirements such as *Federal Information Security Management Act of 2002* (FISMA)[32] privacy reporting. The Office also conducts privacy reviews of Office of Management and Budget (OMB) 300 budget submissions, and supports Component privacy officers and PPOCs to ensure that privacy compliance requirements are met.

The Privacy Office's publication and revision of privacy compliance documentation, integration of compliance processes into Department processes, engagement with program managers at the early stages of program development, and strong relationship with stakeholders throughout the Department demonstrate a mature privacy compliance framework. Some examples from this reporting period include:

- The Chief Privacy Officer initiated a process to review and enhance the PIA guidance and template. The goal is to create a document that is more streamlined and that still provides transparency and in-depth information to the public about DHS's programs. The Office is working with the Component privacy offices to develop new guidance which may result in a new PIA template.

[32] 44 U.S.C. § 3541

- The Office published four PIAs related to the DHS Data Framework, describing the scalable information technology program that will support advanced data capabilities under formal governance processes. These PIAs are: the DHS DATA Framework PIA[33], the Cerberus Pilot,[34] the CEI Prototype,[35] and the Neptune Pilot.[36]
- At the end of June 2014, the Department's FISMA privacy score showed that 84 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 94 percent of required SORNs had been completed.
- During the reporting period, the Department approved eight Computer Matching Agreements (CMA). The Privacy Act requires CMAs when there is a comparison of two or more automated systems of records for the purpose of verifying the eligibility for cash or in-kind federal benefits. Additional information on CMAs is included in Appendix C.
- In partnership with CRCL and OGC, the Office conducted quarterly reviews of CBP's and the TSA's real-time, threat-based intelligence scenarios run by the Automated Targeting System (ATS), to ensure that privacy, civil rights, and civil liberties protections were in place. ATS is an intranet-based enforcement and decision support tool used by CBP to improve the collection, use, analysis, and dissemination of information collected to target, identify, and prevent terrorists from entering the United States. The Privacy Office reviewed the intelligence scenarios four times during the reporting period.
- The Compliance Team, in coordination with the Chief Information Security Officer (CISO), developed a new compliance review framework for the National Institute of Standards and Technology (NIST) privacy controls. The privacy controls became effective on April 1, 2014.[37]

As of June 2014, the Department had a FISMA score of 84 percent for PIAs for required FISMA-related IT systems, and 94 percent for SORNs.

[33] *See* "Privacy Impact Assessment for the DHS Data Framework," November 6, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-dhsdataframework-11062013.pdf.
[34] *See* "Privacy Impact Assessment for the Cerberus Pilot, "November 22, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-cerberus-nov2013.pdf.
[35] *See* "Privacy Impact Assessment for the Common Entity Index Prototype (CEI Prototype)," September 26, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-cei-pilot-_09262013.pdf.
[36] *See* "Privacy Impact Assessment for the Neptune Pilot," September 25, 2013. Available at: http://www.dhs.gov/sites/default/files/publications/privacy-pia-dhs-wide-neptune-09252013.pdf.
[37] *See* National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 30, 2013. Available at: http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf.

The Privacy Office publishes new and updated PIAs on its website at www.dhs.gov/privacy. During the reporting period, the Chief Privacy Officer approved 56 new or updated PIAs. Figure 4 illustrates the number of approved PIAs completed by Component during this reporting period.[38]

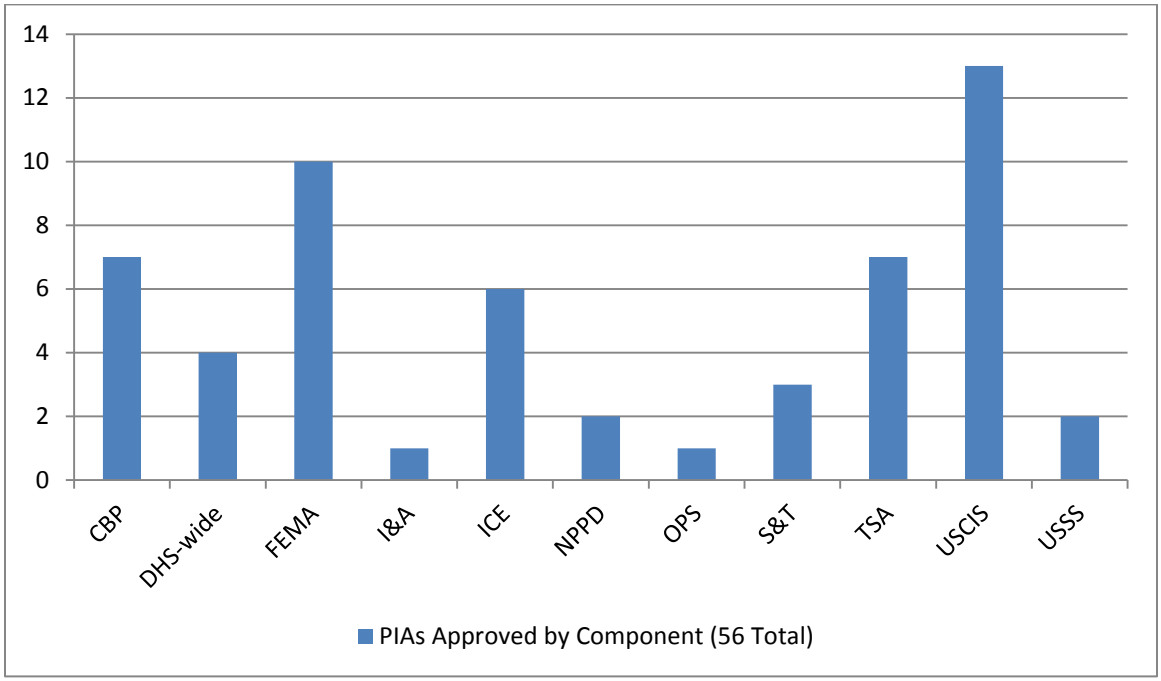


Figure 4: Number of Approved PIAs by Component during the Reporting Period

[38] This represents the total number of new or updated PIAs that were approved by the Chief Privacy Officer during the reporting period. Appendix D provides a list of approved PIAs that were published during the reporting period. A number of PIAs were approved, but not published, during the reporting period. This may occur for two different reasons: (1) the PIA was deemed to contain sensitive information (such as Law Enforcement Sensitive or otherwise classified material) and accordingly the entire document or selected portions were withheld from publication; or (2) publication of the PIA did not occur in time for the close of the reporting period. Information relating to PIAs approved but not published during the reporting period due to sensitive or classified content is being provided to Congress in a separate annex to this report. Approved PIAs published after June 30, 2014, will be included in the Privacy Office 2015 Annual Report, and made available at www.dhs.gov/privacy.

The following are five key PIAs approved during this reporting period:

- DHS/TSA/PIA-041 Pre✓™ Application Program[39]

Background: TSA conducts security threat assessments on individuals who apply to TSA for enrollment into the TSA Pre✓™ Application Program. Program participants are eligible to receive expedited screening at participating airport security checkpoints.

Purpose: TSA conducted this PIA because PII is collected for the conduct of the security threat assessment. (*September 4, 2013)*

- DHS/S&T/PIA-028 Air Entry/Exit Re-Engineering Project[40]

Background: 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 S&T to test various biometric verification systems for effectiveness and efficiency.

Purpose: This PIA addresses the privacy risks and mitigation strategies associated with the testing phase of these biometric systems. *(May 28, 2014)*

- DHS/ALL/PIA-046-1-3 DHS Data Framework[41]

Background: DHS is developing the DHS Data Framework, which is a scalable information technology (IT) program with built-in capabilities to support advanced data architecture and governance processes. This program will alleviate mission limitations associated with stove-piped IT systems that are currently deployed across multiple operational components in DHS. It will also enable more controlled, effective, efficient use and sharing of available homeland security-related information across the DHS enterprise and, as appropriate, the U.S. Government while protecting privacy. DHS is developing three systems to test different capabilities needed to implement the program: the Neptune Pilot, the CEI Prototype, and the Cerberus Pilot. Each of these systems has a separate PIA.

Purpose: DHS published these PIAs because the DHS Data Framework uses PII collected from members of the public using information technology. These PIAs cover the overall approach and vision for the program. As DHS develops the DHS Data Framework, these PIAs will be updated. (*2013)*

[39] http://www.dhs.gov/publication/dhstsapia-%E2%80%93-041-tsa-pre%E2%9C%93%E2%84%A2-application-program.
[40] http://www.dhs.gov/publication/air-entryexit-re-engineering-aeer-project.
[41] http://www.dhs.gov/privacy-documents-department-wide-programs.

- DHS/CBP/PIA-018 Aircraft Systems[42]

Background: CBP employs several types of aircraft, including manned helicopters, fixed-wing aircraft, and UAS for border surveillance and law enforcement purposes. These aircraft are equipped with video, radar, and/or other sensor technologies to assist CBP in patrolling the border, conducting surveillance as part of a law enforcement investigation or tactical operation, or gathering raw data that may assist in emergency response. Video, images, and sensor data collected through these aircraft systems alone cannot be used to identify a person, but they may later be associated with a person as part of a law enforcement investigation or encounter with CBP officers or agents.

Purpose: CBP conducted this PIA to evaluate the privacy impact of these technologies. (*September 9, 2013)*

During this reporting period, the Chief Privacy Officer approved and published 19 SORNs, which are listed by Component in Appendix D. Figure 5 illustrates the number of SORNs completed by Component during this reporting period.

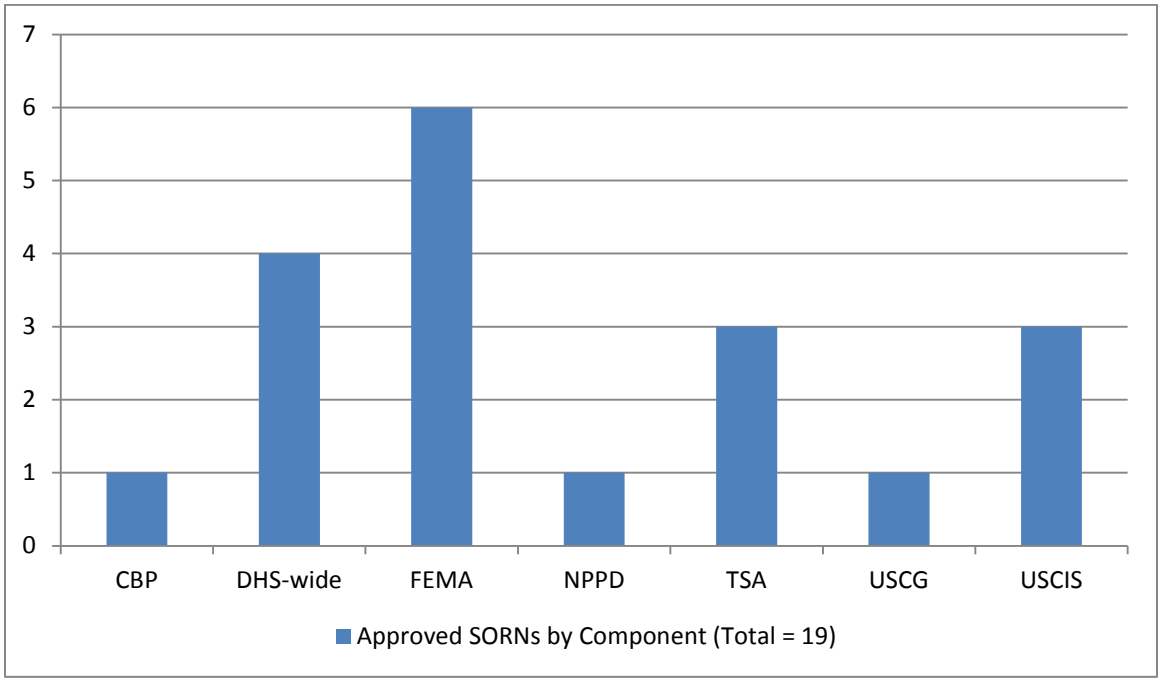


Figure 5: Number of Approved SORNs by Component during the Reporting Period

[42] http://www.dhs.gov/publication/dhscbppia-018-aircraft-systems.

Intelligence Product Reviews

The Privacy Office reviews I&A classified and unclassified briefings, products, reports, directives, and other materials to ensure that the intelligence activities of I&A are conducted in a manner that adequately protects the privacy of individuals. Privacy Office staff apply the FIPPs, pertinent executive orders, and DHS directives during the review process. Staff also participate in the key working groups led by I&A on terrorism-related issues.

During this reporting period, Privacy Office staff reviewed 272 intelligence products and 259 Intelligence Information Reports (IIR).[43] The Office cleared approximately 80 percent of all IIRs and products on first review with only minimal correction. The Privacy Office responded to more than half of all IIRs within two hours; the average response time was within eight hours. Improvements to the IIR and product clearance rates demonstrate an enhanced integration of privacy protections by I&A.

It is not possible to review all the IIRs produced by DHS Components but, working in concert with CRCL, Intelligence Officers, and OGC, the Privacy Office has begun auditing IIRs produced by other DHS Components. In this reporting period, staff audited a random sample of draft TSA Reports Officers IIRs to determine if they raised any privacy issues. The Privacy Office found that all of the audited IIRs were written in a manner that adequately protected individuals' privacy. The Privacy Office intends to continue auditing other Component's IIRs as resources permit.

Privacy Office Staff also participate in the key working groups led by I&A on terrorism-related issues, and have been particularly active in the Combatting Violent Extremism Working Group (CVEWG) during the last year. The CVEWG produced several training videos for first responders, all of which Privacy Office staff helped edit. Privacy Office staff reviewed every minute of the recordings, requesting redactions or blurring of faces as necessary.

Privacy Office staff continue to be actively involved in the Reports Officer Management Council (ROMC), which guides the development of Reports Officers (RO) throughout DHS, and assists in the creation of policy related to drafting and disseminating IIRs. In addition to crafting a complete process for certifying ROs, the ROMC is tackling direct dissemination of IIRs by DHS Components, and levels of classification of DHS IIRs. The ROMC revised and updated the training modules for ROs early in 2014.

[43] IIRs contain "raw" intelligence information that is shared within the IC and state and local partners for informational purposes. The information has not been evaluated or analyzed.

Freedom of Information Act (FOIA) Compliance

FOIA requests:[44] As has been the case for several years, DHS continues to receive the largest number of FOIA requests of any federal department or agency in each fiscal year, receiving almost 30 percent of all requests submitted to the Federal Government in FY 2012. In FY 2013, the Department received an unprecedented number of FOIA requests — 231,534 in total — an increase of 18 percent from FY 2012's total of 190,589. DHS processed 204,332 requests in FY 2013, a decrease of one percent from 205,895 in FY 2012.

FOIA backlog: In last year's report, DHS highlighted a 33 percent decrease in the backlog. In FY 2013, however, the backlog increased from 28,553 to 51,761 due in part to the record-setting number of requests received. Components that process requests seeking immigration-related records (e.g., copies of the alien file, entry/exit records, detention, and deportation records) have the largest backlogs in the Department, with CBP, ICE, NPPD, and USCIS comprising 95 percent of the total DHS backlog. The Department continued to take a multi-pronged approach to reduce its backlog, including the deployment of contractors and Privacy Office staff to the Components with the largest backlogs. Privacy Office staff also met with Component FOIA Officers and officials from other federal agencies to learn how technology, training, and staff development can help reduce the backlog, particularly through day-to-day case management. The Chief Privacy Officer and Deputy Chief FOIA Officer closely monitors the Department's caseload.

FOIA oldest requests and appeals: In FY 2013, DHS set a goal to close the Department's 10 oldest requests and appeals pending, as reported in the previous fiscal year. DHS met its goal and closed the 10 oldest pending requests through more robust oversight of departmental FOIA processing, the hard work of Component FOIA staff, consistent monitoring of FOIA-related performance measures, and a sustained effort toward closing the oldest requests in the backlog throughout the Department's 19 FOIA Components. This was possible, in part, due to the Chief FOIA Officer and General Counsel's formal adoption of a policy to reassign certain complex appeals to United States Coast Guard Administrative Law Judges for processing[45] on a reimbursement basis.

A centralized appeal liaison in the Privacy Office facilitates coordination, tracking, and reporting, and serves as a resource for participating Component offices and public inquiries. Through the collaborative efforts of Component FOIA Officers' timely provision of FOIA administrative files for review, and leveraging qualified staff available for appeal adjudication, the total number of pending appeals for participating Components steadily decreased from 201 at the end of FY 2010 to 24 at the end of FY 2013.[46]

[44] For efficiency, Departmental data reflects the reporting period used in the *Freedom of Information Act Annual Report.*

[45] Chief FOIA Officer and General Counsel Memorandum, "Reassignment of Certain Freedom of Information Act (FOIA) Appeals to United States Coast Guard Administrative Law Judges," July 8, 2011, available at http://www.dhs.gov/publication/reassignment-certain-freedom-information-act-appeals-united-states-coast-guard.

[46] In 2012, FEMA opted not to renew the Memorandum of Understanding (MOU) with the ALJs.

FOIA operations:[47] As mentioned in last year's report, the Privacy Office and several of the Component FOIA offices deployed a new electronic monitoring, tracking, and redacting commercial off-the-shelf web application solution to streamline the processing of requests and appeals under FOIA and the Privacy Act.[48] Currently five of the seven DHS Components and seven of the 19 DHS Headquarters departments are using the web application. As a result, DHS has seen numerous benefits, including: (1) increased productivity; (2) enhanced accuracy in reporting statistics, tracking cases, and better data integrity; and (3) improved interoperability and standardization of the FOIA process across the Department. During this reporting period, the Privacy Office enhanced the web application's functionality to allow for document sharing, consultations, and referrals within the system. Also new this year is the Advanced Document Review, a de-duplication capability that allows FOIA staff to upload e-mail correspondence files and de-duplicate the correspondence based on a comparison process performed by the application.

Online FOIA: In March 2014, the Privacy Office deployed a consolidated web-based form[49] on its public facing FOIA website allowing requesters to submit their requests to the Department and its Components. Detailed information explains how to submit a request and information on where to direct it, while a link off the index page enables requesters to check the status[50] of submitted requests.

FOIA Systems of Records Notice updated: In January 2014, the Chief Privacy Officer signed and updated "Department of Homeland Security/ALL – 001 Freedom of Information Act and Privacy Act Records System of Records," (1) to reflect a change in the location of records, to include the use of electronic FOIA tracking systems by DHS and its Components; (2) to provide additional routine uses to permit additional sharing; and (3) to update categories of records to include responses to requests. DHS added Routine use L, which permits DHS to share the information as follows: "To National Archives and Records Administration, Office of Government Information Services (OGIS), to the extent necessary to fulfill its responsibilities in 5 U.S.C. § 552(h), to review administrative agency policies, procedures, and compliance with FOIA, and to facilitate OGIS's offering of mediation services to resolve disputes between persons making FOIA requests and administrative agencies."

[47] More detailed information on FOIA operations can be found in the *2013 Chief Freedom of Information Act Officer Report to the Attorney General of the United States*.
[48] 5 U.S.C. § 552a.
[49] http://www.dhs.gov/dhs-foia-request-submission-form.
[50] http://www.dhs.gov/check-status-your-foia-request.

IV. Oversight

The Office's FY 2012-2015 Strategic Plan includes five strategic goals:

Privacy Office Strategic Goal 4 (Oversight): *Conduct robust oversight on embedded privacy protections and disclosures in all DHS activities.*

The Privacy Oversight Team is responsible for several Office functions that logically follow from the Privacy Office's core responsibility to ensure that Department programs and systems comply with DHS privacy policy: PCRs, privacy investigations, privacy incident response, and privacy complaint handling and redress. Combining these complementary functions into one team strengthens the Office's oversight role throughout DHS.

Privacy Compliance Reviews

Consistent with the Privacy Office's unique position as both an advisor and an oversight body for the Department's privacy-sensitive programs and systems, the Office designed the PCR to improve a program's ability to comply with assurances made in PIAs, SORNs, and formal information sharing agreements. The Office conducts PCRs of ongoing DHS programs in collaboration with program staff to ascertain how required privacy protections are being implemented, and to identify areas for improvement.

PCRs may result in recommendations to a program, updates to privacy documentation, informal discussions on lessons learned, or a formal internal or publicly available report.

During this reporting period, the Privacy Office completed a sixth PCR for the Department's use of social media for situational awareness (National Operations Center (NOC) Publicly Available Media Monitoring and Situational Awareness Initiative) and had two active PCRs in progress: a review of CBP's Analytical Framework for Intelligence (AFI), and a review of NPPD's implementation of recommendations included in the 2012 PCR for the EINSTEIN Program.[51]

As noted in last year's Annual Report, the Privacy Office introduced a self-audit certification process for the NOC Publicly Available Media Monitoring and Situational Awareness Initiative, as a result of the NOC's history of consistent and positive performance during five previous PCRs. This year's full PCR followed a successful self-audit by the NOC in March 2013.

The Office continued to provide guidance on conducting PCRs to other federal agencies in an effort to foster adoption of the PCR process throughout the federal privacy community, both informally through consultation with colleagues on the CIO Council Privacy Committee and in public settings. A session on how to conduct PCRs was included in the Privacy Office's Annual Privacy Workshop for federal employees on June 10, 2014. The Privacy Oversight Team is committed to assisting other agencies as they strengthen their privacy programs by including PCRs in their oversight toolkits.

U.S. - EU Passenger Name Record (PNR) Agreement

On July 8 and 9, 2013, the Deputy Chief Privacy Officer led a joint review with the European Commission of DHS compliance with the *Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security* dated December 8, 2011. Following the review, the European Commission published its mostly favorable findings on November 27, 2013, and included four recommendations. Since that time, the Privacy Office has overseen implementation of Privacy Office and European Commission recommendations to improve compliance with the Agreement and/or privacy compliance documents.

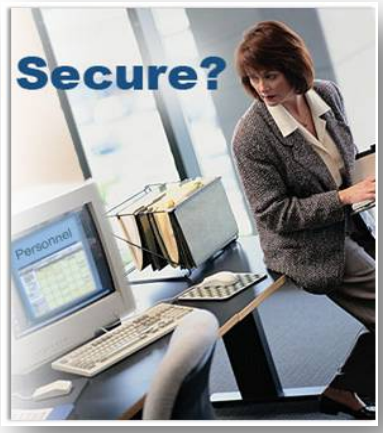
[51] The results of the PCRs for the NOC Publicly Available Media Monitoring and Situational Awareness Initiative and for the EINSTEIN Program are included in public reports available at www.dhs.gov/privacy.

As of July 1, 2014, DHS has implemented all of the Privacy Office recommendations and two of the four European Commission recommendations. The Chief Privacy Officer informed the European Commission of the status and provided updates on the two remaining recommendations. The Privacy Office closely monitors implementation of the remaining recommendations and remains engaged with the Components as DHS continues to comply with the terms of the Agreement. The next joint review is planned for the second quarter of 2015.

Investigations

During this reporting period, the Privacy Office continued to monitor implementation of recommendations it issued in two previous investigations that led to findings of non-compliance with DHS privacy policy.[52] One of these investigations involved a Component's use of social media for operational purposes without appropriate oversight or protections for the collection and use of PII, which led to the issuance of a Department-wide Directive 110-01, *Privacy Policy for Operational Use of Social Media*.[53] The Privacy Office is actively involved in reviewing all DHS Components' proposed uses of social media to ensure that the privacy protections required by the Directive are implemented.

The second investigation concerned a DHS Component's information sharing pilot with an external agency that failed to comply with DHS privacy and information sharing policy and the Privacy Act. With Privacy Office guidance, the Component has developed its own privacy directive, which includes provisions that require all information sharing agreements to be implemented in a privacy-protective manner consistent with Departmental information sharing policy and privacy policy.



Privacy Incident Handling

The Privacy Office manages privacy incident response for the Department and is the author of the *DHS Privacy Incident Handling Guidance* (PIHG),[54] the foundation of DHS privacy incident response. Office staff works to ensure that all privacy incidents are properly reported, investigated, mitigated, and remediated as appropriate for each incident, in collaboration with the DHS Security Operations Center (SOC), Component privacy officers and PPOCs, and DHS management.

[52] Section 802 of the of the 9/11 Commission Act expanded the authorities and responsibilities of the Chief Privacy Officer by adding investigative authority, the power to issue subpoenas to non-federal entities, and the ability to administer oaths, affirmations, or affidavits necessary to investigate or report on matters relating to responsibilities under Section 222 of the Homeland Security Act. *See* 6 U.S.C. § 142.
[53] The Directive is available at http://www.dhs.gov/sites/default/files/publications/privacy/Directive_110-01_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf.
[54] The PIHG is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.

During this reporting period, 773 privacy incidents were reported to the DHS SOC, an increase of 18 percent from the last reporting period. The Department investigated, mitigated, and closed 696 (90 percent) of those privacy incidents. Figure 6 shows the number (and percent of total) of reported DHS privacy incidents by type of incident. Figure 7 shows the number (and percent of total) of reported DHS privacy incidents by Component.

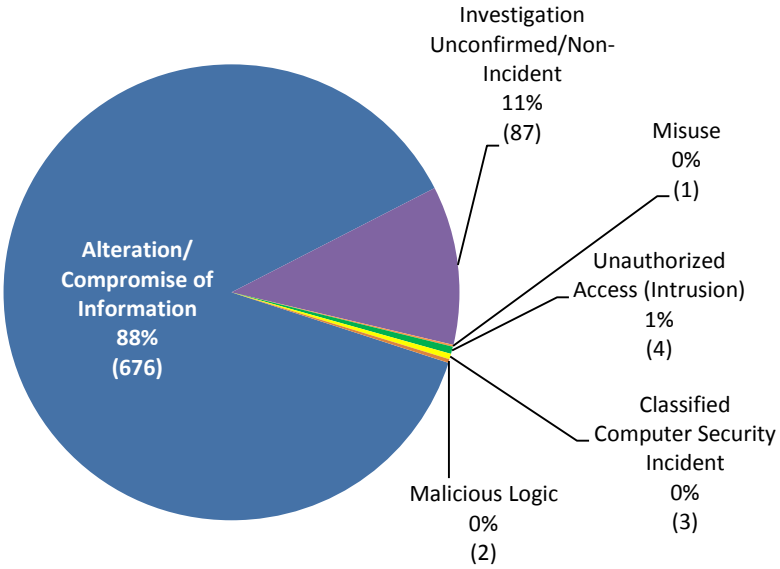


Figure 6: Percentage and Number of DHS Privacy Incidents by Type
July 1, 2013 - June 30, 2014 (total = 773)[55]

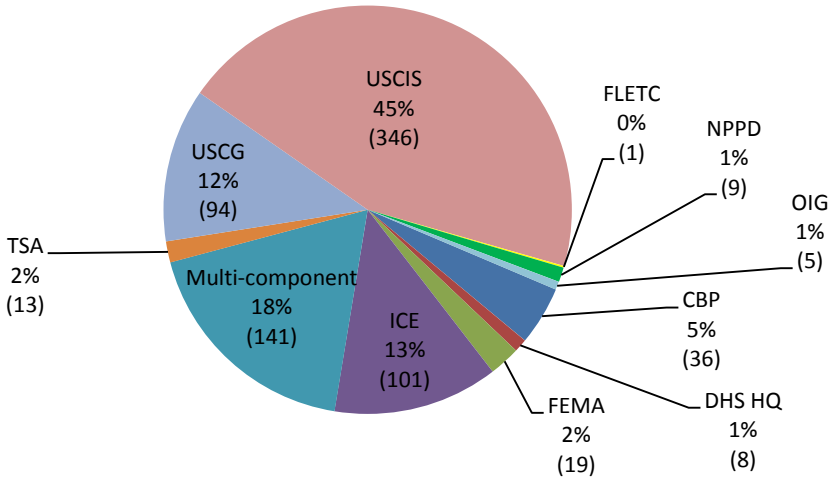


Figure 7: Percentage and Number of DHS Privacy Incidents by Component
July 1, 2013 - June 30, 2014 (total = 773)[56]

[55] Definitions of the categories of privacy incidents are detailed in NIST Special Publication 800-61 (Rev. 1), *Computer Security Incident Handling Guide*, available at http://csrc.nist.gov/.

During this reporting period, the Oversight Team continued its efforts to reduce privacy incidents and to ensure proper incident handling procedures. The Team:

- responded to a major privacy incident affecting personnel throughout the Department by sending out notices to all impacted staff, standing up a call center to handle all inquiries, and guiding the remediation effort.
- disseminated a customizable tip sheet entitled *What You Need to Know About E-mailing Sensitive Personally Identifiable Information (PII)* to all PPOCs. This customizable tip sheet, first in a series from the DHS Privacy Office, is intended to be distributed to Department staff as a reminder of their responsibilities to protect PII when e-mailing within and outside of the DHS network;
- hosted the fifth annual DHS Core Management Group Meeting in September 2013, during which stakeholders met with the Deputy Chief Privacy Officer to discuss privacy incidents and incident handling procedures;
- held Privacy Incident Handling Quarterly Meetings in February and April 2014, providing an opportunity for Component privacy officers, PPOCs, and DHS SOC managers to share best practices and provide feedback on privacy incident management, mitigation, and prevention;
- conducted six site visits to DHS Components to discuss their privacy incident handling procedures and make recommendations for improvement;
- presented on privacy incident handling best practices at two conferences for Federal Government personnel; and
- provided guidance on privacy incident handling to staff at the Departments of Energy and Commerce.

Privacy Complaint Handling and Redress

The Privacy Office is responsible for ensuring that the Department has procedures in place to receive, investigate, respond to, and provide redress for complaints from individuals who contend that the Department has failed to comply with the requirements of the Privacy Act. U.S. citizens, Lawful Permanent Residents, visitors to the United States, and aliens may submit privacy complaints to the Department.[57] The Privacy Oversight team also reviews and responds to privacy complaints referred by employees throughout the Department or submitted by other government agencies, the private sector, or the general public. DHS Components manage and customize their privacy complaint handling processes to align with their specific missions and to comply with Department complaint handling and reporting requirements. Between June 1, 2013, and May 31, 2014, the Department received 3,627 privacy complaints and closed 3,714.

[56] "Multi-component" incidents are incidents that involve more than one DHS Component.

[57] The Department accepts complaints from non U.S. Persons – in other words, persons who are not U.S. citizens or Lawful Permanent Residents – pursuant to the DHS Mixed System Policy set out in *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons*, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf. The Mixed Systems Policy is discussed in Section II.B of the Privacy Office's 2011 Annual Report to Congress, available at http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacy_rpt_annual_2011.pdf.

Figure 8 shows the categories and disposition of privacy complaints the Department received between June 1, 2013 and May 31, 2014.[58]

Section 803 of the *9/11 Commission Act of 2007* and OMB Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* [59] require that the Department report quarterly to Congress on privacy complaints received and their disposition. Section II of this report includes additional information on the Privacy Office's public reporting responsibilities.

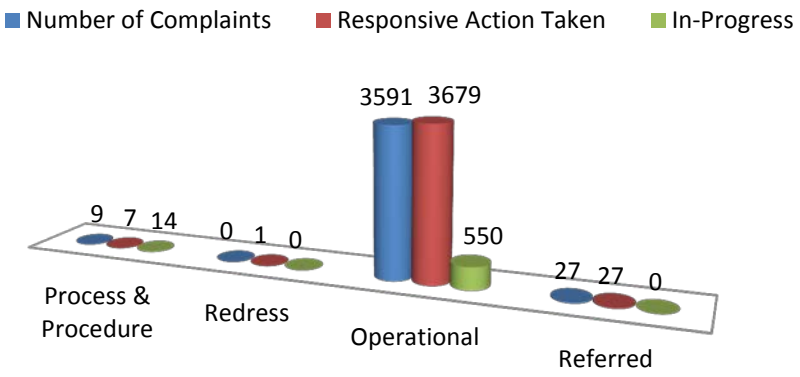


Figure 8: Privacy Complaints Received by DHS June 1, 2013 – May 31, 2014[60]

Illustrative examples of privacy complaints submitted to the Department are included in the Privacy Office's Section 803 Reports.[61]

Privacy Act Amendment Requests

The Privacy Act permits an individual to request amendment of his or her own records.[62] As required by *DHS Privacy Policy Guidance Memorandum 2011-01, Privacy Act Amendment Requests*, Component privacy officers and FOIA Officers are responsible for tracking all Privacy Act Amendment requests and reporting the disposition of those requests to the Privacy Office.[63] The Privacy Oversight Team serves as the repository for those statistics. During the reporting

[58] The quarterly reporting period from June 2014 through August 2014 was ongoing at the close of the reporting period for this Annual Report. Statistics on privacy complaints submitted before June 2014 are provided in the Privacy Office's Section 803 Reports, available at http://www.dhs.gov/files/publications/editorial_0514.shtm. For efficiency, the data reflects the reporting period used in the Section 803 Reports.
[59] OMB Memorandum M08-21 is available at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-21.pdf.
[60] The totals represented include complaints from previous periods that have not yet been resolved. The categories of complaints are defined in OMB M-08-21 and included in the Privacy Office's Section 803 Reports.
[61] Available at http://www.dhs.gov/files/publications/editorial_0514.shtm.
[62] 5 U.S.C. § 552a(d)(2).
[63] http://www.dhs.gov/xlibrary/assets/privacy/privacy-policy-guidance-memorandum-2011-01.pdf.

period the Office received no Privacy Act Amendment requests and DHS Components received 120 requests. Figure 9 shows Privacy Act Amendment Requests received by DHS during the reporting period by Component and disposition.

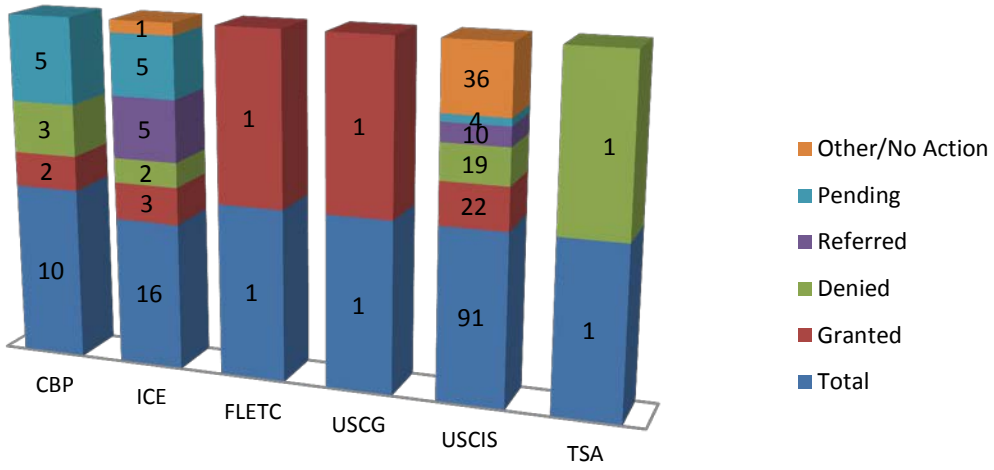


Figure 9: Privacy Act Amendment Requests by Component and Disposition July 1, 2013 - June 30, 2014[64]

Non-Privacy Act Redress Programs

DHS also provides redress for individuals impacted by DHS programs through a number of other mechanisms, including:

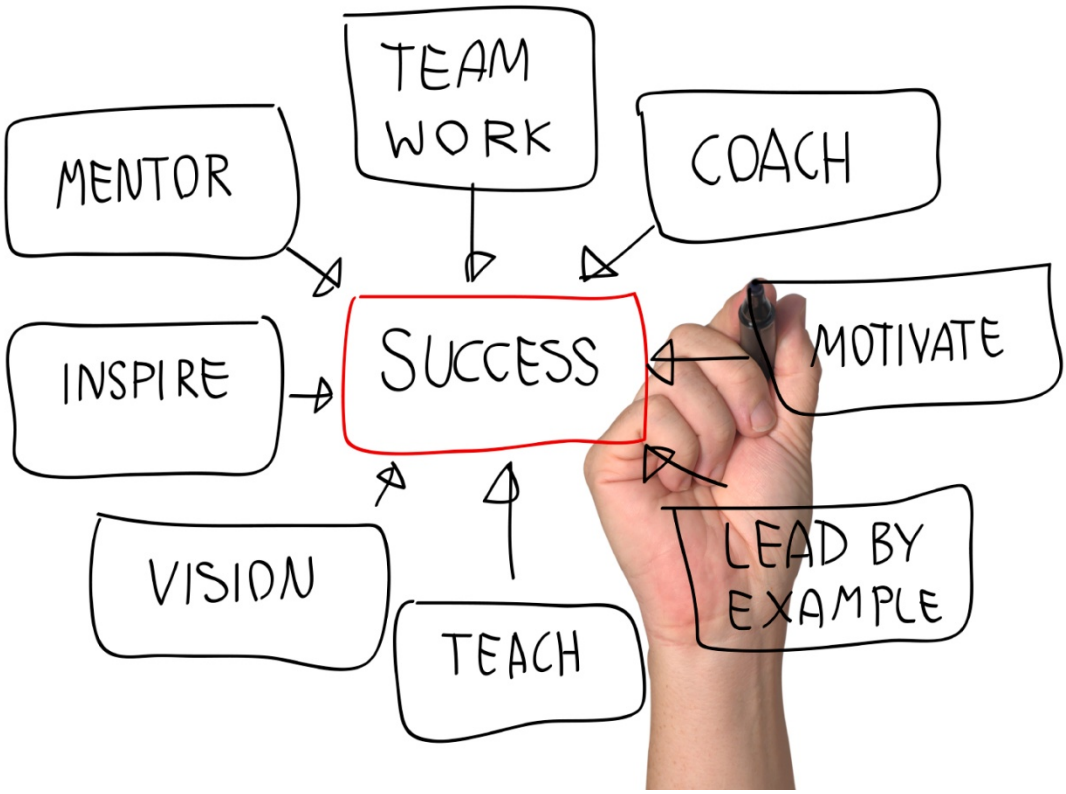
- **Traveler Redress Inquiry Program (DHS TRIP)**. DHS TRIP offers one-stop redress services to the public by providing a centralized processing point for individual travellers to submit redress inquiries. Redress was developed to assist individuals who believe they have been incorrectly denied boarding, or identified for additional screening, or encounter problems at customs and immigration points of entry into the country. In the reporting period July 1, 2013, through June 30, 2014, DHS TRIP received 18,561 requests for redress, with an average response time (from the time of first submission to final resolution) of approximately 66 days.
    - The Chief Privacy Officer is a member of the DHS TRIP Advisory Board. Redress inquiries alleging non-compliance with DHS privacy policy are reviewed by the Privacy Office Oversight Team, and are either referred to the relevant Component, or are handled by the Office, as appropriate.

[64] The total number of ICE Privacy Act Amendment Requests is less than the sum of the individual dispositions because ICE accounted for the closure of four requests that were opened in previous reporting periods.

- **NPPD/OBIM[65] Redress Program.** OBIM maintains biometric information that is collected in support of DHS missions. One of the main goals of the redress program is to maintain and protect the integrity, accuracy, privacy, and security of the information in its systems.
    - OBIM responded to 161 redress requests during the reporting period.

- **Transportation Sector Threat Assessment and Credentialing Redress.** TSA's Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) conducts security threat assessments and completes adjudication services in support of TSA's mission to protect U.S. transportation systems from individuals who may pose a threat to transportation security. OLE/FAMS provides daily checks on over 15 million transportation sector workers against federal watch lists. OLE/FAMS provides a redress process that includes both appeals and waivers for transportation sector workers who feel that they were wrongly identified as individuals who pose a threat to transportation security. Typical redress requests have involved documentation missing from initial submissions, immigration issues, or requests for waivers of criminal histories. During the reporting period, OLE/FAMS granted 8,057 appeals and denied 481. Additionally, OLE/FAMS granted 2,246 waivers and denied 547.

[65] In March 2013, the *Consolidated and Further Continuing Appropriations Act,2013* transferred the legacy US-VISIT overstay analysis mission to ICE and the entry/exit policy and operations to CBP. The Act also transferred the program's biometric identity management functions to OBIM, a newly created office within NPPD.



V. Workforce Excellence

The Office's FY 2012-2015 Strategic Plan includes five strategic goals:

Privacy Office Strategic Goal 5 (Workforce Excellence): *Develop and maintain the best privacy and disclosure professionals in the Federal Government.*

Workforce Development Activities

The Privacy Office has dual responsibilities for preserving privacy and promoting transparency within DHS. Both are important principles to uphold in government, and require first-class expertise and unyielding professionalism from the entire workforce. The Privacy Office maintains these high standards through extensive training and professional development, both in-house and with other centers of excellence for privacy and transparency. During the reporting period, the Office invested in training to promote greater understanding of FOIA and Privacy Act requirements, as well as to broaden staff expertise in other mission areas, such as procurement, cybersecurity and information technology.

Part of the Office's commitment to workforce excellence is its significant emphasis on developing leaders who can promote the mission of the Privacy Office more effectively across the five DHS mission areas. To that end, the office has invested in leadership training for employees at all levels of seniority and experience.

In order to leverage the deep expertise embedded across the Department's privacy and transparency communities, the Privacy Office has actively promoted developmental assignments and rotational job opportunities, both within the Office and in partnership with other DHS Components. The Office actively recruited high caliber employees from DHS Components who can make substantial contributions in a headquarters environment. Similarly, key Privacy Office staff have been sought out and competitively selected by DHS Components and other federal and municipal agencies to assume leadership positions. In addition, to continue growing a pool of talented privacy and transparency professionals, the Office recruited student interns from colleges and universities who have made substantive contributions to a wide range of office responsibilities.

Office Efficiency and Sustainability

Identifying ways to improve efficiency and reduce operating costs continues to be a major focus for the Privacy Office. Personnel costs represent 75 percent of the Office's enacted FY14 budget, so efficient stewardship of all office resources is imperative. The Privacy Office has worked to carefully balance available resources with the staffing levels needed to meet the Office's mission. However, as salary and other recurring costs increase annually through normal inflation, resources are not available to fill all existing vacancies within the Office.

During the reporting period, Office leadership pursued several avenues for cutting costs and improving efficiency, for example, eliminating onsite contractor support, expanding the use of in-house training, and reducing the use of office supplies. Similarly, the Office has taken steps to contribute to the Department's sustainability by reducing its physical footprint and costs associated with office space. In addition, the Office utilized no-cost government facilities to host all of its internal and external training events, as well as to operate the public meetings of its federal advisory committee. The Office conserved additional resources by eliminating the use of print services in favor of electronic publication of all public reports.

Through improved efficiency, management of technology, reduced physical space requirements, and better leveraging of internal resources, the Office has sustained its long-term ability to carry out its mission.

VI. Component Privacy Programs and Operations

DHS has a strong, dedicated network of Component privacy officers and PPOCs who work with the Privacy Office to ensure that Department activities incorporate privacy from the earliest stages of system and program development. Component privacy officers and PPOCs provide operational insight, support, and privacy expertise for Component activities. This section of the report highlights the activities of Component privacy offices during this reporting period.

Federal Emergency Management Agency (FEMA)

FEMA coordinates the Federal Government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all domestic disasters, whether natural or man-made, including acts of terror. The FEMA Privacy Office (FEMA Privacy) sustains privacy protections and minimizes privacy impacts on FEMA's constituents, while supporting the agency in achieving its mission.

During this reporting period, FEMA Privacy engaged in the following significant activities:

Privacy Policy Leadership and Development

- Developed and issued the first comprehensive FEMA Privacy Program Manual on June 6, 2014, to fully implement the FEMA Privacy Program Directive published during the last reporting period.
- Collaborated on the development of FEMA Recovery Policy 9420.1 *Secure Data Sharing.* Issued on September 13, 2013, this policy outlines, among other things, rules for maintaining, retrieving, and disseminating PII with partners.
- Continued to represent privacy interests on FEMA's Strategic Leadership Steering Committee and Integrated Project Team for FEMA's agency-wide Workplace Transformation Initiative. With the agency's immersion in workplace transformation, there has been increased interest in how information is being handled, shared, stored, and protected in the new FEMA open environment. As a result, the culture of privacy awareness has shifted and the FEMA Privacy Officer is consistently consulted on senior level strategic initiatives and newly proposed policy that may impact personal privacy.
- Continued to serve on FEMA's Policy Working Group to ensure that all policies are developed to minimize privacy impacts.
- Continued to leverage the FEMA Privacy Council, which includes PPOCs from every FEMA directorate and office to serve as liaison officers with the FEMA Privacy Office, and ensure that critical privacy issues are communicated, directed, reported, and otherwise shared among appropriate leadership, system owners, program managers, Information System Security Officers (ISSO), and Information System Security Managers (ISSM) to further the FEMA privacy mission.
- Expanded the FEMA Privacy Office Disaster Operations Branch to include two additional Cadre of On-call Employee privacy analyst positions. The Disaster Operations Branch addresses agency privacy issues and initiatives with a disaster nexus, and implements the

DHS OIG's recommendations resulting from the May 2013 FEMA Privacy Stewardship audit.[66]

Privacy Compliance

- Achieved a FISMA score for SORNs of 94 percent, and a FISMA score of 93 percent for PIAs, during this reporting period.
- Completed or updated 80 PTAs, 10 PIAs, and 6 SORNs during the reporting period.
- Renewed a Computer Matching Agreement with the U.S. Small Business Administration (SBA) that will allow the sharing of information for the purpose of ensuring that applicants for SBA Disaster Loans and FEMA Other Needs Assistance will not receive duplicate benefits for the same disaster. Under the CMA, FEMA and SBA will continue to share data until August 2015.
- Continued and expanded the Privacy Compliance Undocumented System Initiative[67] to complete new or update existing FEMA privacy compliance documentation associated with the agency's inventory of privacy-sensitive systems identified by the DHS/OIG during the FEMA privacy stewardship.

Highlights of privacy compliance documents:
All PIAs and/or SORNs referenced below can be found in Appendix D, as well as on the Privacy Office website at: www.dhs.gov/privacy.

- Published a PIA covering all of the agency's deployment programs for disaster-related personnel.
- Published a PIA for the agency's program for qualifying disaster response and recovery personnel for deployment.
- Published a PIA for the agency's Disaster Reporter Application, a smart-phone application that allows users use any smart phone to upload and transmit photos and text descriptions from the scene of a disaster to the agency. FEMA then displays the information on a public-facing map so it can be viewed for situational awareness and to inform decision making.
- Published a PIA for the agency's IT system that allows disaster applicants to securely access the agency's IT system for disaster assistance application.
- Published a PIA for the agency's updated financial management system that tracks and manages disaster assistance payments and agency programmatic payments.
- Published a SORN to consolidate records into a single system for all disaster-related grant and loan programs, including the public assistance program.
- Published a SORN to consolidate National Flood Insurance Program marketing, insurance policy issuance, and claims processing files into a single system.

[66] http://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-87_May13.pdf.

[67] FEMA's on-going effort to comply with OIG's recommendation to establish privacy compliance around FEMA's inventory of undocumented privacy-sensitive systems began during the last reporting period.

Privacy Incident Response and Mitigation

- Developed and issued FEMA Form 654-0-2, *Statement to the FEMA Privacy Office* in May 2014 to allow FEMA to gather written statements or reports and signed attestations from individuals in response to privacy inquiries, incidents, and concerns. FEMA's new form contributes to a more formalized and streamlined investigation and fact-gathering process.
- Implemented a *Protection of Privacy Sensitive Information* clause, which has been inserted into numerous FEMA procurement contracts, in an effort to ensure contractor employment suitability and accountability for agency PII data and information.

Privacy Training and Outreach

- Initiated a FEMA National Capital Region (NCR)-wide privacy training and site risk analysis campaign in support of the agency's Workplace Transformation Initiative to co-locate FEMA personnel within the NCR, and reduce the agency's office space footprint.
- Developed a Privacy Compliance Foundations training module and presented it to ISSOs, 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 the above referenced information professionals, limit review iterations, and expedite the clearance and approval process.
- Continued to hold quarterly collaboration meetings and targeted training sessions for FEMA Privacy Points of Contacts to ensure there is a FEMA-wide focus on accurate and timely incident reporting, enforcement of mandatory annual privacy training, and identifying and reporting privacy sensitive systems that require privacy assessment and/or documentation.
- Continued to conduct privacy awareness training for all new FEMA employees in the NCR.
- 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.

Privacy Oversight

- Developed and implemented a FEMA Privacy Compliance Site Assessment framework, tool, and training module. This internal tool will be used to provide evidence based privacy counsel and advice to FEMA operations. The Privacy Compliance Site Assessment framework was designed with privacy compliance reviews of field operations in mind, but will be used at all FEMA locations. The Privacy Compliance Site Assessment framework was rolled out in Winchester, Virginia, followed by privacy reviews in Anniston, Alabama, Atlanta, Georgia, and Baton Rouge and New Orleans, Louisiana.
- Closed the last of four DHS OIG recommendations from the May 2013 FEMA Privacy Stewardship audit to assess unauthorized systems and complete appropriate privacy compliance documentation.

Federal Law Enforcement Training Centers (FLETC)

FLETC is an interagency law enforcement organization that trains state, local, rural, tribal, territorial, and international law enforcement agencies. Since FLETC was established in 1970, it has trained over one million law enforcement officers and agents.

During the reporting period, the FLETC FOIA & Privacy Program Office engaged in the following significant activities:

Privacy Policy Leadership and Development

- Continued to work closely with IT colleagues to ensure that privacy compliance is embedded in IT development.

Privacy Compliance

- Achieved a FISMA score of 100 percent for both PIAs and SORNs during the reporting period.
- Completed or updated 5 PTAs during the reporting period.

Privacy Incident Response and Mitigation

- Coordinated with the DHS Privacy Incident Response Team to respond to a multi-Component privacy incident involving the exposure of Sensitive PII. Worked closely with FLETC Human Capital Division to ensure accurate and timely communications.

Privacy Training and Outreach

- Worked with FLETC's Protocol and Communications Office on social media issues and associated privacy concerns. Reviewed and edited the FLETC Social Media Directive.
- Updated the Privacy Act release form to a plain English format and posted to the FLETC FOIA/Privacy Act web page.
- Reviewed and provided privacy language for a FLETC draft Administrative Investigation Directive.
- Provided content for the FLETC Twitter account how to protect PII and Sensitive PII at work, at home, and while on business travel.

National Protection and Programs Directorate (NPPD)

The mission of NPPD is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. During this reporting period, NPPD privacy staff supported the NPPD Federal Protective Service (FPS), OBIM, Office of Infrastructure Protection, Office of Cyber Infrastructure Analysis and Office of Cybersecurity and Communications, and engaged in the following significant activities to promote and protect privacy while supporting critical mission operations:

Privacy Policy Leadership and Development

- Issued a Delegation of Authority to prepare and respond to requests for Privacy Act information in support of civil or criminal law enforcement activity covered under Section (b)(7) of the Privacy Act.
- Issued Instruction 4400.1, *Access to and Use of Social Media*, which prescribes the procedures NPPD employees and contractors must follow when utilizing approved social media sites for the purpose of communications and public outreach.
- Participated as a key member of the working group that drafted the Chief Information Officer Council's paper, *Privacy Best Practices for Social Media,*[68] published in July 2013.

Privacy Compliance

- Achieved a FISMA score of 100 percent for both PIAs and SORNs during this reporting period.
- Completed or updated 36 PTAs, 2 PIAs, and 1 SORN during the reporting period.
- In addition to completing privacy compliance documentation, NPPD completed 8 Privacy Act Statements and 3 Paperwork Reduction Act packages.

Highlights of privacy compliance documents:
All PIAs and/or SORNs referenced below can be found in Appendix D, as well as on the Privacy Office website at: www.dhs.gov/privacy.

- FPS published a Dispatch and Incident Record Management Systems PIA Update. This update provides additional transparency into how case management data is used, including using CBP's TECS system as an investigative case management tool, as well as incorporating limited case management data into the DHS Pattern Information Collaboration Sharing System.
- FPS conducted PTAs of two agreements involving access to or sharing of closed circuit television data for the purpose of protecting federally-owned or leased facilities supported by the FPS.
- IP published an update to the Chemical Facilities Anti-Terrorism Standards Personnel Surety PIA. This update details the privacy impact associated with the Chemical Facility Anti-Terrorism Standards Personnel Surety Program, and the required security assessments

[68] https://cio.gov/wp-content/uploads/downloads/2013/07/Privacy-Best-Practices-for-Social-Media.pdf

performed by high-risk chemical facilities in fulfillment of Risk-Based Performance Standard #12 (6 C.F.R. § 27.230(a)(12)). The PIA describes the procedures for submitting PII on individuals impacted by this program to NPPD, and also describes NPPD's uses of that PII. NPPD updated the PIA to account for changes to the program since the publication of the program's original PIA on May 4, 2011.

Privacy Incident Response and Mitigation

- To help prevent privacy incidents, OBIM conducted inspections to remind employees to keep their workstations locked or log out while they are away from their offices. Reminder cards were left at unattended, unlocked workstations.

Privacy Training and Outreach

- The Privacy team received the directorate's Empowerment Award, formal recognition of the team's efforts to ensure that all employees are empowered to safeguard PII and make informed decisions in areas where there may be an impact on an individual's personal privacy.

NPPD Privacy conducted the following training and awareness events:

- Hosted quarterly privacy awareness events:
  - December 2013: Privacy and Technology Workshop for employees and contractors in the National Capital Region. Participants received technology demonstrations and learned about topics such as privacy, IT security, biometrics, and tools to protect from malware, cyber stalking, and spear phishing.
  - March 2014: Two-day *Privacy Training Days* event, with sessions held at four directorate office locations, targeting employees and contractors in the National Capital Region. All 128 attendees received credit for completing their annual privacy training requirement.
  - June 2014: In order to reach employees outside of the National Capital Region, hosted two webinar versions of the training offered during the last quarter's *Privacy Training Days* event, attracting 93 participants.

- All NPPD personnel completed the mandatory annual online course, *Privacy at DHS: Protecting Personal Information*.

- 440 employees completed the FPS Privacy Requirements for Operational Use of Social Media online training course, which is a prerequisite for access to social media for the purpose of criminal investigations or law enforcement intelligence activities in support of protection of federally-owned or leased facilities.

- Delivered both online and in-person training to the Office of Security and Compliance staff on accessing social media tools for the purpose of handling administrative investigations. FPS staff received similar training geared toward the use of social media for criminal investigations and law enforcement intelligence activities.

- Embedded privacy into the acquisition process by providing a series of briefings to Contracting Officer Representatives across the directorate, covering privacy considerations for acquisitions, as well as core provisions for incorporation into NPPD acquisition vehicles to protect privacy. The Privacy Team also participated in Contractor Officer Representative quarterly meetings to provide refresher briefings and discuss lessons learned.

- Held three training sessions for the Information Technology contractors supporting OBIM's systems operations.

- Provided specialized training to Office of Infrastructure Protection employees on the protection of stakeholder contact information.

- Co-hosted training sessions with CRCL on privacy, civil rights and civil liberties considerations that employees and contractors should be aware of when developing and reviewing external products. These training sessions followed the release of an external product checklist used to help employees evaluate privacy, civil rights and civil liberties concerns. One training session was also recorded and published so that field employees can take the training in a self-paced fashion.

- Provided a virtual privacy briefing to the regional division directors and their immediate staff for the FPS Resource Management divisions, including financial management, project management, personnel security, administrative services, and information technology.

Assisted the NPPD FOIA Office and OGC FPS legal advisors in providing a one-day FOIA and Privacy Act (PA) training seminar in Alexandria, Virginia for FPS FOIA/PA liaison officers and alternates located in FPS' 11 regions. In addition, NPPD routinely publishes articles and tips in employee newsletters, such as the *Privacy Update*, *NPPD VISION*, and *InsideOBIM*, to help foster awareness of emerging privacy issues.

NPPD also conducted the following outreach activities:

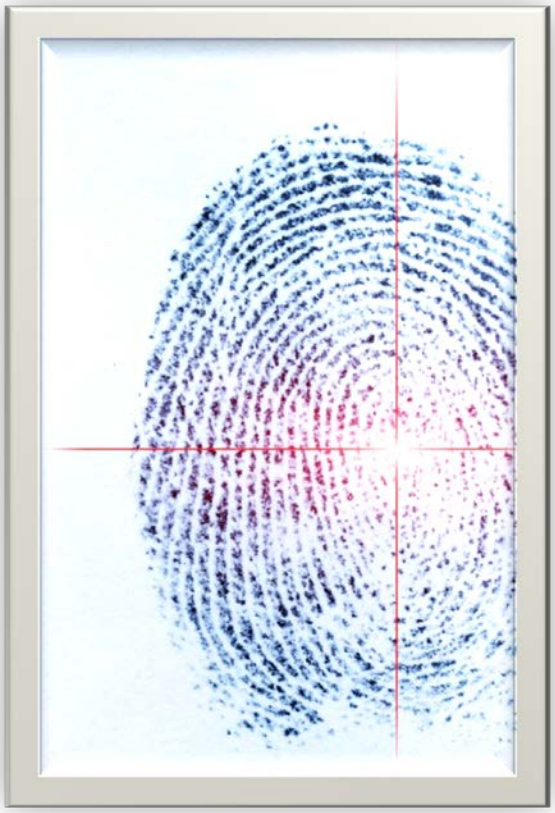
- On September 19, 2013, the Senior Privacy Officer moderated a panel at OBIM's workshop, *Improving Public Perceptions of Biometrics*, held at the Biometric Consortium Conference in Tampa, Florida.

- On December 13, 2013, an NPPD senior privacy analyst spoke on a social media panel at the IAPP Government Practical Privacy Series in Washington, DC.

- On June 10, 2014, two NPPD privacy analysts participated in the DHS Privacy Workshop by leading break-out teams for an interactive privacy compliance walkthrough focused on applying recently learned privacy compliance principles to adjudicating a PTA.

Privacy Oversight

- NPPD conducted 141 privacy reviews as part of the Information Technology Acquisition Review process. Through this process, the directorate ensures that all Information Technology acquisitions in excess of $2.5 million include core privacy provisions whenever contracted services may involve access to PII.
- Through workgroup participation, NPPD Office of Privacy has been actively involved in implementing requirements under EO-13636, and participated in the DHS Privacy Office assessment of NPPD activities under EO-13636 and PPD-21.
- NPPD Office of Privacy conducted four Quarterly Privacy Reviews on National Cybersecurity & Communications Integration Center and the United States Computer Emergency Readiness Team's (US-CERT) handling of PII during this reporting period. Two major deliverables that came out of this work are (1) the Cybersecurity and Communications Quarterly Privacy Review of PII Handling Procedures document that outlines roles and responsibilities during the Quarterly Privacy Review process and (2) role-based training, a collaborative effort by NPPD Privacy, the Office of General Counsel, and US-CERT. The training follows US-CERT Standard Operating Procedures for handling PII and targets US-CERT staff engaged in cyber threat operations.



Office of Intelligence and Analysis (I&A)

I&A is responsible for collecting, analyzing, producing, and disseminating intelligence and information needed to keep the homeland safe, secure, and resilient. I&A provides intelligence support across the full range of DHS mission areas to DHS and its Components, state, local, tribal, and territorial governments, and the private sector. The I&A Privacy Officer ensures that I&A intelligence activities are conducted in a manner that adequately protects individuals' privacy through a variety of activities that are highlighted below. In addition, the I&A Privacy Officer serves as the Intelligence Oversight Officer, with responsibilities to ensure compliance with EO 12333, U.S. Intelligence Activities, and other intelligence-related authorities in preparing and disseminating intelligence products. These responsibilities intersect with privacy compliance because intelligence authorities include specific requirements for handling the PII of U.S. persons.

Privacy Policy Leadership and Development

- Maintained a privacy blog for a multi-agency information sharing environment that explains the FIPPs and the requirements of the Privacy Act to blog readers.
- Participated in the DHS Privacy, Civil Rights, and Civil Liberties Working Group on Unmanned Aircraft Systems to examine the privacy implications of expanded use of UAS.
- Joined other privacy colleagues in developing processes and procedures to implement the President's cybersecurity initiative embodied in EO 13636 and PPD21.
- Helped create DHS Directive 262-05, Information Sharing and Safeguarding, which establishes standards and assigns responsibilities to implement an insider threat detection and prevention program pursuant to EO 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, referred to as "The Insider Threat Program." The Program is intended to prevent unauthorized disclosure of classified national security information, deter cleared employees from becoming insider threats, detect employees who pose a risk to classified national security information, and mitigate risks to the security of classified national security information through administrative, investigative, or other responses, while protecting the privacy and civil rights and civil liberties of DHS personnel.
- Participated in the DHS Watchlisting Cell Working Group to help ensure that appropriate privacy protections are embedded in Department watchlisting activities.

Privacy Compliance

- I&A, as an element of the Intelligence Community, is exempt from FISMA reporting requirements.
- Completed 15 PTAs during the reporting period.
- Continued efforts with the SharePoint team to ensure that internal SharePoint sites are appropriately bannered when Sensitive PII is present, and that other privacy requirements are met.
- Published Policy Instruction, IA-801, Producing Privacy Compliant Systems and Processes, which established standards for the completion of privacy compliance documentation for

I&A programs, business processes, and information technology systems that collect, maintain, use, and/or disseminate PII.

Privacy Incident Response and Mitigation

- Helped to mitigate the impact of privacy incidents of varying severity.

Privacy Training and Outreach

- Provided intelligence oversight training to approximately 800 Department personnel. This training includes a discussion of privacy requirements and an explanation of best practices to advance constitutional and statutory protections.
- Trained approximately 200 new personnel.
- Published notices in internal communications to remind personnel about their obligations pursuant to the Privacy Act, especially the need to remain vigilant in protecting PII.

Science and Technology Directorate (S&T)

S&T manages science and technology research to protect the homeland, from development through transition, for DHS Components and first responders. S&T's mission is to strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the homeland security enterprise.

During the reporting period, the S&T Privacy Office (S&T Privacy) engaged in the following significant activities:

Privacy Compliance

- Achieved a FISMA score of 100 percent for both PIAs and SORNs during this reporting period.
- Completed or updated 28 PTAs and 3 PIAs during the reporting period.

Highlights of privacy compliance documents:
All PIAs and/or SORNs referenced below can be found in Appendix D, as well as on the Privacy Office website at: www.dhs.gov/privacy.

- Published the Air Entry Exit Reengineering PIA. The program tests, evaluates, and develops options to implement congressionally-mandated biometric entry and exit requirements.

These requirements will improve the screening and verifying of the identities of foreign nationals arriving at or departing from United States airports. S&T Privacy has worked with CBP and the DHS Privacy Office to identify and mitigate the privacy risks associated with this project through the PIA, and with civil rights and civil liberties groups to promote transparency.

- Published the Facial Recognition Data Collection Project PIA Update to address the privacy risks and mitigation strategies associated with the S&T-funded Pacific Northwest National Laboratory project that collected facial video data from volunteers at the Toyota Center in Kennewick, Washington.

Privacy Incident Response and Mitigation

- Partnered with the DHS Privacy Incident Response Team to respond to a potential privacy incident involving the potential exposure of Sensitive PII, and addressed questions and concerns from S&T employees potentially affected by the incident.

Privacy Training and Outreach

S&T Privacy develops and delivers annual, bi-weekly orientation, and ad-hoc privacy awareness training for all S&T staff and contractors:

- Annual online mandatory Privacy Awareness Training.
- Bi-weekly training for new S&T employees and contractors.
    - S&T privacy attends the bi-weekly S&T New Employee Orientation to provide basic information on how to safeguard PII, identify privacy incidents, and who to contact for advice when dealing with privacy sensitive information.

S&T Privacy provided additional privacy training at these conferences and events:

- Annual DHS Privacy Workshop
- Department of Veterans Affairs, Privacy Awareness Week
- International Association of Privacy Professionals, Practical Privacy Series
- American Conference Institute, Privacy & Security Conference
- Department of Transportation, Privacy Summit
- Netherlands Bi-lateral Science & Technology Delegation
- DHS S&T Industry Day: Data Privacy Technologies Research and Development

Transportation Security Administration (TSA)

TSA is responsible for protecting the nation's transportation systems to ensure freedom of movement for people and commerce. TSA is most visible through its airport security screening efforts, but is also responsible for the security of other modes of transportation, including highways, maritime ports, railways, mass transit, and pipelines.

During the reporting period, the TSA Privacy Office (TSA Privacy) engaged in the following significant activities:

Privacy Policy Leadership and Development

- Reviewed 243 pending contract actions to implement PII safe handling and breach remediation requirements when necessary, and ensure that any other privacy compliance requirements implicated by the contract are completed.
- Provided continuous advice and oversight on passenger screening protocols, security technology initiatives, and information sharing initiatives.
- Provided advice on Secure Flight risk-based screening proposals and the TSA Pre✓™ rollout.

Privacy Compliance

- Achieved a FISMA score of 90 percent for PIAs, and 98 percent for SORNs during this reporting period.
- Completed or updated 30 PTAs, 7 PIAs and 3 SORNs during the reporting period.

Highlights of privacy compliance documents:
All PIAs and/or SORNs referenced below can be found in Appendix D, as well as on the Privacy Office website at: www.dhs.gov/privacy.

- Published a PIA Update for the Crew Member Self Defense Training Program, a voluntary self-defense training course for U.S. commercial and cargo air carrier crew members. The program trains crew members on how to defend the flight deck against acts of criminal violence or air piracy. TSA updated this PIA to reflect that it will: (1) collect information from crew members solely through electronic means; and (2) conduct personnel security suitability checks on American Association of Community College Site Coordinators so that they may be granted access to an existing secure TSA web-based system in order to process registrations on behalf of crew members.

- Published a PIA Update for the Secure Flight program. The program screens aviation passengers and certain non-travelers before they access airport sterile areas or board aircraft. TSA updated this PIA to reflect the following operational changes: (1) the addition of Known Traveler populations to TSA Pre✓™; (2) the use of Secure Flight to screen passengers on certain government operated flights; and (3) the use of intelligence-driven flight by flight risk assessments to identify passengers and non-traveling individuals who require either enhanced

screening or are eligible for expedited screening. The changes are anticipated to result in the identification of more passengers who are eligible for expedited screening in airports with TSA Pre✓™ lanes.

- Published a PIA Update for the Enterprise Performance Management Platform that assists in performing security management functions using data associated with security, equipment, and screening processes from TSA's security activities. The Platform maintains PII on members of the public in excess of basic contact information. TSA updated this PIA to reflect the following: 1) the inclusion of the Visible Information Management System, a data management module within the Enterprise Performance Management Platform framework, that supports the Visible Intermodal Prevention and Response Program; 2) the transfer of payroll transactions for Transportation Security Officers from the Performance Management Information System to the Airport Information Management System; and 3) the storing of PII on individuals identified in the Terrorist Screening Database as posing a threat to transportation or national security.

- Published a PIA for TSA's Pre✓™ Application Program. TSA conducts security threat assessments on individuals who apply to TSA for enrollment into this program which provides eligible participants with expedited screening at participating airport security checkpoints. TSA conducted this PIA because PII is collected during the security threat assessment.

Privacy Incident Response and Mitigation

The TSA Privacy Office developed a simplified procedure for securing credit monitoring services for privacy incidents that affect a small group, and coordinated programmatic acquisition approvals to implement the procedures across TSA. The new procedures permit more timely delivery of credit monitoring services and permit greater flexibility in responding to privacy incidents involving only a few victims.

Privacy Training and Outreach

- Reached out to a variety of privacy and civil liberties groups and thought leaders, to include the American Civil Liberties Union, the Center for Democracy & Technology, the Cyber Privacy Project, and the Liberty Coalition to discuss TSA's risk-based security and Pre-Check initiatives, along with the Secure Flight program.
- Presented on "How to Build Privacy into your Governmental Organization" at both the IAPP Practical Privacy seminar and the Federal Aviation Administration's Privacy Conference.
- Created a simplified guidance document for all DHS Component Privacy Offices to use for completing annual OMB Exhibit 300 budget reviews for IT systems over $100,000.
- Trained staff at TSA's Office of Intelligence & Analysis, Office of Human Capital, Office of Law Enforcement (Personnel Security Division), and Office of Information Technology (ISSOs) on PII safe handling.
- Presented training on "Privacy at Work & Home" during the TSA Power of Learning series, and privacy training as an integral part of the Sensitive Security Information webinar for Sensitive Security Information Coordinators.

- Published a factsheet about protecting PII while teleworking and distributed the brochure throughout TSA.
- Disseminated broadcast e-mail messages related to information protection, including how to secure medical information, the privacy risks of networked copiers, and ways to limit PII collection on TSA web sites.

Privacy Oversight

- Incorporated privacy compliance elements within audit functions performed by the TSA Management Control Oversight Program for internal controls at all TSA offices. The elements include periodic self-inspection of hard-copy and electronic data security, and document destruction practices.
- Conducted annual reviews of 43 programs to ensure that the existing PIAs adequately represented their activities and associated privacy protections.

United States Citizenship and Immigration Services (USCIS)

The USCIS Office of Privacy (USCIS Privacy) works diligently to promote a culture of privacy across USCIS, to sustain privacy protections in USCIS programs, directorates, and initiatives, and to enhance the privacy awareness of employees and contractors by developing policies, conducting privacy trainings and outreach opportunities, reducing privacy incidents, and participating in privacy-related working groups.

During the reporting period, USCIS Privacy engaged in the following significant activities:

Privacy Policy Leadership and Development

USCIS Privacy issued the following guidance/reminders:

- Published an update to the USCIS Privacy Act contract clause, dated September 15, 2013. This clause replaced the current Privacy Act clause for contracts that involve the collection, processing, use, maintenance, or storage of PII maintained in a Privacy Act system of records.
- Developed additional language referencing PII for the mid-year and Annual Performance Evaluation Guidance for leadership and management.

Privacy Compliance

- Increased its FISMA score for PIAs from 87 percent during the previous reporting period to 94 percent for this reporting period. Also increased its FISMA score for SORNs during this reporting period to 100 percent from 97 percent last year.
- Completed or updated 131 PTAs, 13 PIAs, and 3 SORNs during the reporting period.

Highlights of privacy compliance documents:
All PIAs and/or SORNs referenced below can be found in Appendix D, as well as on the Privacy Office website at: www.dhs.gov/privacy.

- Published a PIA for the Case and Activity Management for International Operations system. The system is a secure, web-based case management application designed to facilitate the effective and efficient processing of immigration applications and petitions received or adjudicated by overseas offices and domestic branches of USCIS IO Headquarters. This PIA discusses the USCIS system used to support its international offices and evaluates the privacy risks and mitigation strategies built into the system. USCIS conducted this PIA because the system collects and uses PII.
- Published a PIA Update for the Enterprise Citizenship and Immigration Services Centralized Operational Repository (repository), which streamlines access to relevant information necessary to administer the Immigration and Nationality Act. This repository consolidates information collected during the adjudication of applications and petitions for immigration benefits. USCIS updated and reissued this PIA to clarify the repository's functionalities, and to discuss all source systems and interconnected systems.

Privacy Incident Response and Mitigation

- Managed and mitigated 383 of the reported 398 incidents that involved the possible loss, compromise, or unauthorized disclosure of PII. Mitigation is ongoing for the remaining 15 incidents.
- Published the Privacy Incident Management Standard Operational Plan, dated May 13, 2014.

Privacy Training and Outreach

- Hosted the Fourth Annual Privacy Awareness Day on June 3-5, 2014. Events were held at headquarters and in the regional offices.
- Published a specialized training module entitled "Privacy Compliance Boot Camp" to provide guidance on how to complete privacy compliance documentation.
- Hosted a new **"***Town Hall Forum***"** for the Orlando Field Office to address questions from employees and contractors on how to assess, report, mitigate, and prevent a privacy incident.
- Published a privacy awareness/educational article entitled "*Protecting PII on your Shared Drives*" in the California Service Center's monthly newsletter.
- Published a quarterly newsletter to convey the importance of properly disposing of PII and Sensitive PII, as well as guidance on reporting privacy incidents, in addition to privacy news, tips, and guidance for safeguarding PII.
- Published multiple privacy tips on the USCIS intranet, highlighting topics that focused on the appropriate use, access, sharing, and disposing of PII.

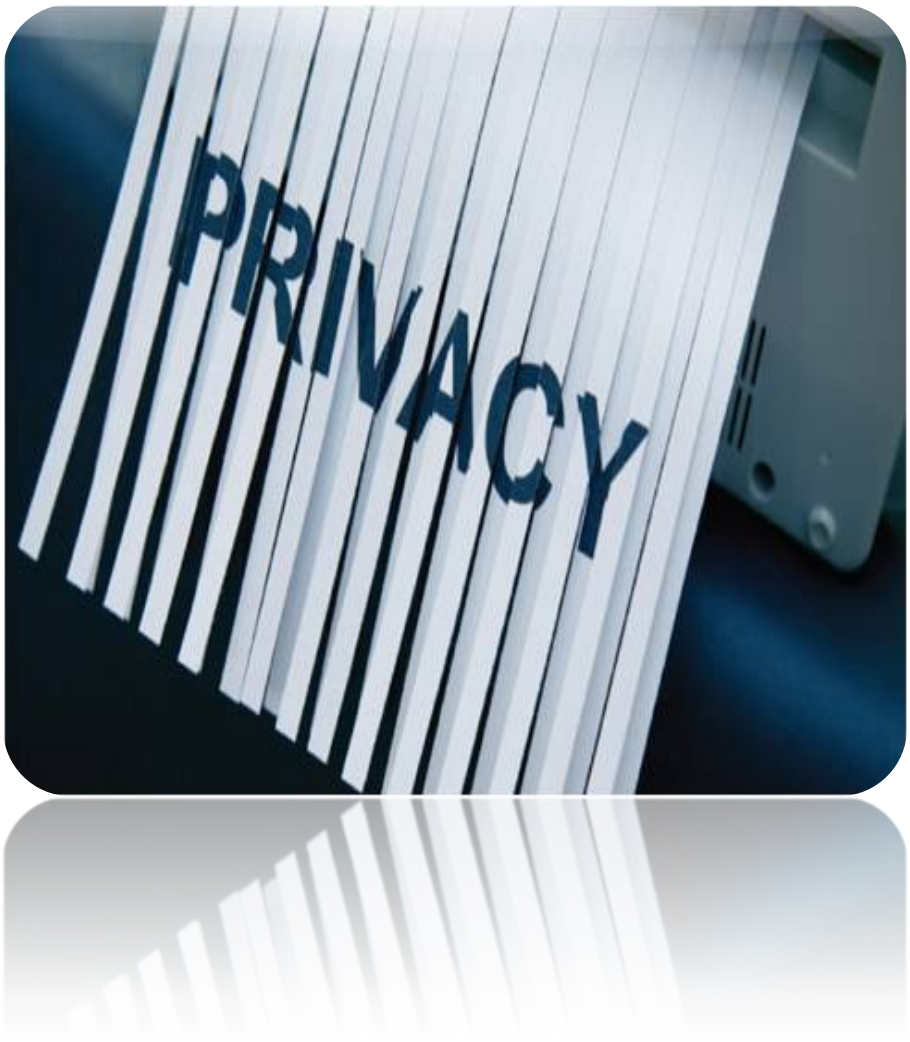
Provided training for the following:

- Mission support specialists on how to safeguard PII and respond to privacy incidents.
- ISSOs on the security authorization process and how privacy fits into this process.
- Central and Southeast regional district directors and field office directors on the USCIS Office of Privacy's policies, procedures and processes; the purpose and function of the regional privacy program; and how the regional privacy officer can assist leadership in ensuring compliance with privacy regulations, policies and procedures.

Privacy Oversight

- Conducted 60 site visits and privacy risk assessments of various USCIS facilities.
- Conducted four privacy audits of directorates located at USCIS headquarters, in conjunction with the Office of Security and Integrity and the Office of Information Technology.
- Reviewed and assessed 133 contract statements of work to determine whether a Privacy Act notification clause and/or training requirements needed to be met.
- Continued to enhance and expand the USCIS privacy program through: (1) promotion of a culture of privacy awareness with federal privacy laws, DHS regulations, and policies through education and awareness, training, and on site audits; (2) working collaboratively with the USCIS program and operational offices, along with the Chief Information Officer, ensuring USCIS technology systems have appropriate privacy protections implemented

according to privacy laws, regulations, and DHS policy; and (3) developing and distributing internal policy and guidance to promote, improve, and strengthen the operationalization of privacy processes according to privacy laws and regulations.



United States Coast Guard (USCG)

The Coast Guard began in 1790 with a plan to govern the maritime commerce of our fledgling Nation. In that year, Congress authorized the construction of ten cutters to improve enforcement of customs duties and tonnage taxes. Since then, Coast Guard responsibilities have continuously expanded to encompass every aspect of maritime governance. Today, as the Nation's maritime first responder, the USCG ensures the safety, security, and stewardship of the Nation's waters by protecting those on the sea, protecting the Nation against threats delivered by sea, and protecting the sea itself.

During this reporting period, the USCG Privacy Office engaged in the following significant activities:

Privacy Policy Leadership and Development

- Promulgated a Component-wide message emphasizing the importance of safeguarding Sensitive PII, citing current policy/procedures on e-mail, shared computer network drives, and computer-readable extracts.
- Collaborated with Human Resources (HR) to include PII violations as a punishable offense in the USCG Civilian Personnel Actions Manual.
- Partnered with the Office of Health, Safety, and Work-Life to develop a USCG mobile application providing real-time information to Coast Guard families on the availability and accessibility of individual and family support services.
- Teamed with Quality Performance Improvement and Information Assurance Divisions and disseminated a message to medical personnel on the importance of safeguarding PII and protected health information.
- Developed numerous Privacy Act Statements and safeguarding procedures associated with the USCG Civilian Employee Voluntary Separation Incentive Payment and Voluntary Early Retirement Authority programs.
- Collaborated with USCG Information Assurance and presented viable options to the USCG Commodore of Auxiliary on how to safely e-mail data from commercial e-mail accounts to the DHS/USCG domain.
- Developed an official Privacy Act data cover sheet that personnel may use to label documents containing PII.

Privacy Compliance

- Maintained a FISMA score of 97 percent for PIAs and 98 percent for SORNs during this reporting period.
- Completed 58 PTAs and one SORN during the reporting period.
- Conducted a biennial review of all USCG System of Record Notices.

Privacy Incident Response and Mitigation

On October 11, 2013, USCG Cyber Command discovered a USCG server transmitting unencrypted PII to a commercial server. It was found that an external website (i.e., dirauxam.org) was used to retrieve PII from the server in order to create USCG Auxiliary identification cards. Access was halted and the server was taken off-line. Notification letters were sent to all impacted current and former USCG Auxiliarists, offering one year of free credit monitoring/ identity theft counseling.

Privacy Training and Outreach

USCG Privacy conducted two privacy awareness forums with USCG ISSOs and the Office of Regulations to convey best practices for safeguarding PII, along with updates to the recently revised PTA template.

United States Customs and Border Protection (CBP)

CBP guards the Nation's borders and safeguards the Nation while fostering economic security through lawful international trade and travel. CBP's unique role at the border provides it with access to a broad array of data concerning people and merchandise arriving into and departing from the United States. CBP officials use and share the data for a variety of border security, trade compliance, and law enforcement purposes.

During the reporting period, the CBP Privacy Office (CBP Privacy) engaged in the following significant activities:

Privacy Policy Leadership and Development

- Briefed Senate Judiciary Committee staff on the privacy issues associated with DHS's use of UAS.
- Revised the CBP Management Directive on the Use and Disclosure of ATS Passenger Name Record Data.
- Created a Standard Operating Procedure for information sharing with law enforcement entities.
- Reviewed over 600 one-time requests for information from CBP systems, and issued an authorization memorandum specific to each case. The increase in requests this reporting period reflects the growth in reliance on CBP records to support law enforcement investigations and prosecutions.
- Developed directives on the use of social media and privacy policy generally.

Privacy Compliance

- Devoted significant resources to overseeing proper information sharing with other international, foreign, federal, state, local, and tribal government agencies to ensure that the information shared would be used as described in each system's PIA and SORN.
- Achieved a FISMA score of 49 percent for PIAs and 77 percent for SORNs.
- Completed or updated 41 PTAs, 7 PIAs, and one SORN during the reporting period.

Highlights of privacy compliance documents:
All PIAs and/or SORNs referenced below can be found in Appendix D, as well as on the Privacy Office website at: www.dhs.gov/privacy.

- Published a PIA and SORN for the Customs-Trade Partnership Against Terrorism System. This is a voluntary program in which members agree to provide CBP with information pertaining to their internal analysis, measurement, and monitoring of their cargo supply chains in exchange for greater security and efficiency at U.S. Ports of Entry.

- Published a PIA and SORN for the Global Enrollment System. This system allows CBP to handle the enrollment and vetting processes for trusted traveler and registered traveler programs in a centralized environment. Because individuals who wish to participate in these programs voluntarily provide PII in return for expedited transit, the PIA and SORN discuss

the potential privacy risks associated with the system, and how CBP has employed safeguards to mitigate those risks.

- Published a PIA and SORN for the Intellectual Property Rights e-Recordation and Search Systems. These systems collect, use, and maintain records related to intellectual property rights recordations and their owners. CBP uses this repository of protected trademarks, trade names, and copyrights to provide trade enforcement for these valuable economic assets. The PIA and SORN discuss the potential privacy risks for any collected PII, and how CBP has employed safeguards to mitigate those risks.

Privacy Incident Response and Mitigation

- Managed and continue to mitigate 31 CBP-specific privacy incidents involving potential or actual compromise of PII during the reporting period.
- Continued to advocate for technology solutions to remove Social Security numbers from CBP systems.

Privacy Training and Outreach

- Revised the privacy-related section of the mandatory online training: *IT Security Awareness and Rules of Behavior*.
- Conducted privacy training for CBP senior officials who were appointed privacy liaisons from the offices of IT, Internal Affairs, International Trade, Field Operations, and Border Patrol. The training covered not only how to handle PII, but also the role of senior officials in spreading the culture of privacy throughout CBP. CBP Privacy meets with these liaisons regularly.
- Conducted privacy training for the Office of Field Operations auditors in the National Capital Region.
- Conducted privacy training for officials in CBP Laboratories and Scientific Services at the Federal Law Enforcement Center in Charleston, South Carolina.
- Briefed the CBP attaché to the United Kingdom on CBP privacy and data protection laws and regulations.

Privacy Oversight

In response to last year's OIG audit of CBP's privacy stewardship,[69] CBP reorganized its Privacy Office within the Office of Diversity and Civil Rights, reporting to the Office of the CBP Commissioner. Twelve staff attorneys from the Office of International Trade/Regulations and Rulings were detailed to this new office to provide support for the mission and functions of CBP Privacy, and to train their replacements as they are hired.

[69] U.S. Customs and Border Protection Privacy Stewardship Report: http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-78_Apr12.pdf

United States Immigration and Customs Enforcement (ICE)

ICE is the principal investigative arm of DHS and the second largest investigative agency in the Federal Government. ICE promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

During the reporting period, the ICE Privacy Office (ICE Privacy) engaged in the following significant activities:

Privacy Policy Leadership and Development

- Established a new process whereby the ICE Privacy Office conducts privacy reviews of proposed procurements that involve the collection, maintenance, processing, or use of or access to PII. This process is intended to identify privacy issues prior to contract issuance, and ensure that the appropriate privacy protections are included in contract language.

Privacy Compliance

- Achieved FISMA scores of 83 percent for PIAs and 100 percent for SORNs.
- Completed or updated 34 PTAs, six PIAs, one DHS/ALL PIA, one SORN, one Final Rule, six Disposition PTAs, and 17 Testing Questionnaires during the reporting period.
- Reviewed the DHS Notice of Proposed Rulemaking and Final Rule entitled *Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities* (6 C.F.R. part 115) for privacy compliance. Developed the proposed update to the pertinent Department-wide SORN to support the new collection and dissemination of PII under the Final Rule.

Highlights of privacy compliance documents:
All PIAs and/or SORNs referenced below can be found in Appendix D, as well as on the Privacy Office website at: www.dhs.gov/privacy.

- Published a Final Rule for the Homeland Security Investigations (HSI) Forensic Laboratory (laboratory) SORN. This laboratory is an accredited crime laboratory located within HSI that provides a broad range of forensic, intelligence, and investigative support services for ICE, DHS, and many other U.S. and foreign law enforcement agencies. The SORN provided notice to the public regarding the existence of the Imaged Documents and Exemplars Library, and the Final Rule was published to identify exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

- Proposed an update to the DHS/ALL-020 Internal Affairs System of Records to support ICE's implementation of a Final Rule entitled *Standards to Prevent, Detect, and Respond to Sexual Abuse and Assault in Confinement Facilities* (6 C.F.R. part 115), and to better reflect DHS's internal affairs records systems. The SORN update incorporated ICE's collection, use, maintenance, and dissemination of information related to the Final Rule. The Internal Affairs system of records collects and maintains records relating 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 OIG.

- Published a new PIA for ICE's electronic Travel Document System, which provides an efficient means for ICE personnel to request, and foreign consular officials to review and adjudicate, travel document requests for aliens who have been ordered removed or granted voluntary departure from the United States, but do not possess valid travel documents.

- Published a new PIA for the electronic Health Records System (system), which ICE uses to maintain health records of aliens whom ICE detains for violations of U.S. immigration law. Aliens held in ICE custody in a facility staffed by the ICE Health Services Corps receive medical, dental, and mental health evaluations and treatment depending on the alien's medical condition and length of stay. As the system maintains PII and health information about ICE detainees, ICE conducted this PIA to assess the privacy issues associated with the collection, maintenance, and use of this information.

- Published a new PIA for the FALCON Data Analysis and Research for Trade Transparency System (system), a component system of the larger HSI system environment. This PIA was necessary because the system accesses and stores PII retrieved from data systems owned by DHS and other government agencies, as well as commercially available databases. With the deployment of this system, the legacy system, which served the same function as the newer system, as well as the PIA for the legacy system, was retired.

- Published a PIA update for the Enforcement Integrated Database (database), a shared common database repository for several DHS law enforcement and homeland security applications. This database 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 ICE and CBP. This update addresses plans to further expand criminal history information sharing, to include fingerprints and photographs with foreign countries about their nationals who are being removed from the United States. The sharing of criminal history information will be formalized using a Memorandum of Cooperation signed by DHS and each country that elects to participate in these sharing agreements.

- Published a PIA update for the FALCON Search and Analysis System (system), a consolidated information management system that enables ICE law enforcement and homeland security personnel to search, analyze and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal and administrative laws. This PIA was necessary because the system accesses and stores PII retrieved from DHS, other government agencies, and commercially available databases.

- Published a PIA update for the Immigration and Customs Enforcement Child Exploitation Tracking System (system), which is a centralized information repository that assists law enforcement in conducting child exploitation investigations. The system's database aggregates tips and lead information about Internet-facilitated child sexual exploitation crimes in a single repository; allowing investigators to identify links in otherwise unrelated

matters to reduce redundant investigative work. With this update to the PIA, ICE has expanded the use of this system within DHS to permit select CBP personnel to access and directly query data within the system.

Privacy Incident Response and Mitigation

During the reporting period, there were 134 privacy incidents. The ICE Privacy Office staff resolved 120 of these privacy incidents, taking various steps to mitigate any effects of the incidents and prevent future incidents.

Privacy Training and Outreach

- Conducted New Hire Orientation privacy training sessions for approximately 105 ICE Headquarters employees.
- Conducted five privacy training sessions for SharePoint collaboration site points of contact, training seven ICE employees and contractors.
- Participated in a panel discussion at the DHS Law Enforcement Information Sharing Roundtable on August 20, 2013, addressing the legal and privacy considerations in information sharing.
- Conducted privacy training at the ICE Office of Professional Responsibility, Office of Detention Oversight New Employee Orientation Training on September 25, 2013, on the proper handling of Sensitive PII and privacy incidents.
- Participated as a panelist discussing privacy and policy issues in the law enforcement environment at the 2013 ACT-IAC Executive Leadership Conference on October 28, 2013.
- Provided training and awareness content on privacy and social media issues to all ICE employees during ICE's Cyber Security Month in October 2013.
- Conducted training at the ICE Homeland Security Investigations Basic Intelligence Training Course on January 31, 2014 and April 2, 2014, on the importance of privacy, disclosures under the Privacy Act, properly handling of Sensitive PII, and privacy incidents. Training now occurs quarterly.

United States Secret Service (USSS or Secret Service)

The Secret Service's mission is to safeguard the nation's financial infrastructure and payment systems to preserve the integrity of the economy, and to protect national leaders, visiting heads of state and government, designated sites, and National Special Security Events.

During this reporting period, the USSS FOIA & Privacy Act Program (USSS Privacy) engaged in the following significant activities:

Privacy Policy Leadership and Development

- Engaged in USSS's Information Technology Review Committee's quarterly meetings to identify all newly proposed or operational systems, and facilitated engagements with project managers and program managers to ensure that privacy considerations are embedded in the design of each system.
- Issued an official message to all employees and supervisors reminding employees of the Secret Service privacy policy regarding the use of social media for both law enforcement and non-law enforcement purposes.
- Updated the current USSS Privacy Act directive.
- Created a new directive to provide guidance on the proper handling and safeguarding of PII and Sensitive PII.

Privacy Compliance

- Achieved a FISMA score of 89 percent for PIAs and 86 percent for SORNs.
- Completed or updated 5 PTAs and 2 PIAs during the reporting period.
- Reviewed and drafted Privacy Act statements for new and existing USSS forms and web sites that collect PII.

Privacy Incident Response and Mitigation

Issued official e-mail messages to all USSS employees regarding the importance of safeguarding PII and reporting privacy incidents, and reminding employees of a dedicated phone line and e-mail address for privacy and FOIA-related inquiries and/or comments.

Privacy Training and Outreach

- 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.
- 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.
- Updated compliance training slides and provided training to over 80 employees on July 25, 2013.
- Updated the USSS intranet page to disseminate information to employees about privacy compliance, guidelines, and tools.
- Provided mandatory annual online privacy awareness training to all Secret Service employees and contractors.
- Continued to provide mandatory privacy training on the operational use of social media to employees whose positions require it.
- Designed a comprehensive online training module for the operational use of social media.

The Future of Privacy at DHS

The Privacy Office is entering an extremely challenging period. DHS is building systems and implementing programs to counteract formidable threats and motivated bad actors who are constantly adapting their strategies to disrupt the Nation's physical and cyber security. At the same time, the public expects transparency, and is acutely attuned to any initiatives that infringe on privacy.

The principles of privacy and transparency at DHS are integrally tied to the five homeland security missions outlined in the 2014 Quadrennial Homeland Security Review. These missions, more than ever, are facilitated by the ubiquity and capabilities of computing, and by complex datasets. The technology available to meet DHS's missions is powerful, and looks promising in its potential to make us safer.

The value of technology to identify and share indicators of potential cyber threats or to identify previously unrecognized patterns cannot be understated; but neither should the privacy risks. All of this technology can help achieve a risk-based, non-discriminatory approach to implementing the DHS missions. The Privacy Office will ensure that it is used in a manner that sustains, but does not erode privacy, by embedding privacy at the front-end of these initiatives as well as monitoring the privacy impact throughout their lifecycles.

The pace of technological change demands that DHS respond thoughtfully— with new policies and protections, with greater speed and with fewer resources.

The imperative of the Privacy Office, the wider DHS privacy and FOIA community, and indeed the entire Department—is to stay ahead of these challenges. And, in order to do so, the Privacy Office must remain focused on these priorities:

1. A renewed emphasis on being a responsible steward for the personal data of citizens and non-citizens alike;
2. Critically assessing new systems and programs while working collaboratively with the operators and system designers to develop strong, innovative privacy protections;
3. Expanding our service as a consultative organization that identifies, explores, and develops best practices for privacy and transparency, as we are currently doing with UAS and have done for years with cybersecurity; and
4. Finally, we must continue maturing and strengthening the privacy enterprise by continuing to set and raise the bar for transparency; boosting our engagement with the

privacy community; and modernizing privacy protections in some of DHS's outdated IT systems.

In the future, new threats will emerge, and technology—not yet imagined—may be part of the solution to countering those threats. So we must develop novel uses of information while being mindful of the privacy impact; cultivate new relationships while keeping a collective ear to the ground about how notions of privacy might evolve; and take affirmative measures to protect privacy while explaining those protections to the public—all of which will make privacy professionals even more essential to the missions of DHS.

It is our hope and expectation that in the course of decades to come, the Privacy Office, and the Department as a whole, will be even more widely celebrated in its efforts to preserve American values as DHS works to protect the homeland.

Appendix A – Acronym List

Acronym List	
AFI	Analytical Framework for Intelligence
App	Mobile application
ATS	Automated Targeting System
BTB	Beyond the Border
CBP	United States Customs and Border Protection
CEI	Common Entity Index Prototype
CFO	Chief Financial Officer
CHCO	Chief Human Capital Office or Officer
CIO	Chief Information Officer
CMA	Computer Matching Agreement
CRCL	Office for Civil Rights and Civil Liberties
CVEWG	Combatting Violent Extremism Working Group
CVTF	Common Vetting Task Force
DHS	Department of Homeland Security
DHS TRIP	DHS Traveler Redress Inquiry Program
DOJ	Department of Justice
DPIAC	Data Privacy and Integrity Advisory Committee
EO	Executive Order
FACA	Federal Advisory Committee Act
FBI	Federal Bureau of Investigation
FCC	Five Country Conference
FEMA	Federal Emergency Management Agency
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act of 2002
FLETC	Federal Law Enforcement Training Centers
FOIA	Freedom of Information Act
FPS	Federal Protective Service
FY	Fiscal Year
HR	Human Resources
HSIN	Homeland Security Information Network
HQ	Headquarters
HSI	Homeland Security Investigations
I&A	Office of Intelligence and Analysis
IAPP	International Association of Privacy Professionals
IC	Intelligence Community
ICAM	Identity, Credentialing, and Access Management
ICE	United States Immigration and Customs Enforcement
IdM	Identity Management
IGA	Office of Intergovernmental Affairs

Acronym List	
IGB	International Governance Board
IIR	Intelligence Information Report
ISA-IPC	Information Sharing and Access Interagency Policy Committee
ISAA	Information Sharing Access Agreement
ISCC	Information Sharing Coordinating Council
ISE	Information Sharing Environment
ISP	Internet Service Provider
ISSGB	Information Sharing and Safeguarding Governance Board
ISSM	Information Security System Manager
ISSO	Information Security System Officer
IT	Information Technology
ITF	Integrated Task Force
LESMC	Law Enforcement Shared Mission Command
NCR	National Capital Region
NCTC	National Counterterrorism Center
NIST	National Institute for Standards and Technology
NOC	National Operations Center
NPPD	National Protection and Programs Directorate
NPRM	Notice of Proposed Rulemaking
NSTC	National Science and Technology Council
OBIM	Office of Biometric Identity Management
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OGC	Office of the General Counsel
OGIS	Office of Government Information Services
OIG	Office of Inspector General
OIP	DOJ Office of Information Policy
OLE/FAMS	TSA Office of Law Enforcement/Federal Air Marshal Service
OMB	Office of Management and Budget
OPS	Office of Operations Coordination and Planning
PACT	Privacy Administrative Coordination Team
P/CL	Privacy and civil liberties
PCR	Privacy Compliance Review
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIHG	Privacy Incident Handling Guidance
PLCY	Office of Policy
PNR	Passenger Name Records
PPAT	Privacy Policy and Advocacy Team
PPD	Presidential Policy Directive
PPOC	Privacy Point of Contact

Acronym List

PRA	Paperwork Reduction Act
PTA	Privacy Threshold Analysis
RO	Reports Officer
ROMC	Reports Officer Management Council
S&T	Science and Technology Directorate
SAOP	Senior Agency Officials for Privacy
SAR	Suspicious Activity Reporting
SBA	United States Small Business Administration
SBU	Sensitive but Unclassified
SMOUT	Social Media Operational Use Template
SOC	Security Operations Center
SORN	System of Records Notice
SOP	Standard operating procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration
UAS	Unmanned Aircraft Systems
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

Appendix B – DHS Implementation of the Fair Information Practice Principles (FIPPs)

DHS's implementation of the FIPPs is described below:[70]

Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

Individual Participation: DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

Purpose Specification: DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration.

Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.

Data Quality and Integrity: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.

Security: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

[70] *Privacy Policy Guidance Memorandum 2008-01, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security* (Dec. 29, 2008), available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

Appendix C – Compliance Activities

The Privacy Compliance Process

DHS systems, initiatives, and programs must undergo the privacy compliance process, which consists of completing privacy compliance documentation and undergoing periodic reviews of existing programs to ensure continued compliance.

The Privacy Office, in collaboration with the CIO, Chief Information Security Officer, and Chief Financial Officer (CFO), identifies programs that must be reviewed for privacy compliance through several avenues including:

(1) the FISMA Security Authorization process, which identifies IT systems that must meet privacy requirements under FISMA;

(2) the OMB IT budget submission process, which requires the Privacy Office to review all major DHS IT investments and associated systems on an annual basis, prior to submission to OMB for inclusion in the President's annual budget, to ensure that proper privacy protections and privacy documentation are in place;[71]

(3) CIO IT Program Reviews, which are comprehensive reviews of existing major IT investments and include a check for accurate and up-to-date privacy compliance documentation; and,

(4) PRA processes, which require the Privacy Office to review DHS forms that collect PII to ensure that only the information needed to fulfil the purpose of the collection is required on forms. This review also ensures compliance with the Privacy Act Statement requirement, pursuant to 5 U.S.C. § 552a(e)(3).

Privacy Compliance Documents: Keys to Transparency and Accountability

The DHS privacy compliance documentation process includes three primary documents: (1) the PTA, (2) the PIA, and (3) the SORN. Each of these documents has a distinct function in implementing privacy policy at DHS, but together they further the transparency of Department activities and demonstrate accountability.

PTAs

The first step in the process is for DHS staff seeking to implement or modify a system, program, technology, or rulemaking to complete a PTA. The Privacy Office reviews and adjudicates the PTA. This document serves as the official determination as to whether or not the system, program, technology, or rulemaking is privacy sensitive (i.e., involves the collection and use of PII) and requires additional privacy compliance documentation such as a PIA or SORN.

[71] *See* Office of Management & Budget, Executive Office of the President, OMB Circular No. A-11, Section 300, *Planning, Budgeting, Acquisition, and Management of Capital Assets*, available at http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/s300.pdf.

PIAs

The E-Government Act and the Homeland Security Act require PIAs, and PIAs may also be required in accordance with DHS policy issued pursuant to the Chief Privacy Officer's statutory authority. PIAs are an important tool for examining the privacy impact of IT systems, initiatives, programs, technologies, or rulemakings. The PIA is based on the FIPPs framework and covers areas such as the scope and use of information collected, information security, and information sharing. Each section of the PIA concludes with analysis designed to outline any potential privacy risks identified in the answers to the preceding questions and to discuss any strategies or practices used to mitigate those risks. The analysis section reinforces critical thinking about ways to enhance the natural course of system development by including privacy in the early stages.

If a PIA is required, the relevant personnel will draft the PIA for review by the Component privacy officer or PPOC and Component counsel. Part of the PIA analysis includes determining whether an existing SORN appropriately covers the activity or a new SORN is required. Once the PIA is approved at the Component level, the Component privacy officer or PPOC submits it to the Compliance Team for review and approval. The Chief Privacy Officer conducts a final review before signing. Once approved, PIAs are published on the Privacy Office website, with the exception of a small number of PIAs deemed classified for national security reasons.

PIAs are required when developing or issuing any of the following:

- **IT systems** that involve PII of members of the public, as required by Section 208 of the E-Government Act;
- **Proposed rulemakings** that affect PII, as required by Section 222 (4) of the Homeland Security Act [6 U.S.C. § 142(a)(4)];
- **Human resource IT systems** that affect multiple DHS Components, at the direction of the Chief Privacy Officer;
- **National security systems** that affect PII, at the direction of the Chief Privacy Officer;
- **Program PIAs**, when a program or activity raises privacy concerns;
- **Privacy-sensitive technology PIAs**, based on the size and nature of the population impacted, the nature of the technology, and whether the use of the technology is high profile; and,
- **Pilot testing** when testing involves the collection or use of PII.

SORNs

The Privacy Act requires that federal agencies issue a SORN to provide the public notice regarding PII collected in a system of records. SORNs explain how the information is used, retained, and may be corrected, and whether certain portions of the system are subject to Privacy Act exemptions for law enforcement or national security reasons. If a SORN is required, the program manager will work with the Component privacy officer or PPOC and Component counsel to write the SORN for submission to the Privacy Office. As with the PIA, the Chief Privacy Officer reviews, signs, and publishes all SORNs for the Department.

Periodic Reviews

Once the PTA, PIA, and SORN are completed, they are reviewed periodically by the Privacy Office (timing varies by document type and date approved). For systems that require only PTAs and PIAs, the process begins again three years after the document is complete or when there is an update to the program, whichever comes first. The process begins with either the update or submission of a new PTA. OMB guidance requires that SORNs be reviewed on a biennial basis.[72]

Computer Matching Agreements and the DHS Data Integrity Board

Under *The Computer Matching and Privacy Protection Act of 1988*, which amended the Privacy Act, federal agencies must establish a Data Integrity Board to oversee and approve their use of CMAs.[73] The Chief Privacy Officer serves as the Chairperson of the DHS Data Integrity Board and members include the Inspector General, the Officer for Civil Rights and Civil Liberties, the Office of the Chief Information Officer, and representatives of Components that currently have active CMA in place.[74]

Before the Department can match its data with data held by another federal agency or state government, either as the recipient or as the source of the data, it must enter into a written CMA with the other party, which must be approved by the DHS Data Integrity Board. CMAs are required when there is a comparison of two or more automated systems of records for the purpose of verifying the eligibility for cash or in-kind federal benefits.[75]

Under the terms of the computer matching provisions of the Privacy Act, a CMA may be established for an initial term of 18 months. Provided there are no material changes to the matching program, existing CMAs may be recertified once for a period of 12 months. Thus, the Department must re-evaluate the terms and conditions of long-standing computer matching programs regularly.

[72] Office of Management & Budget, Executive Office of the President, OMB Circular No. A-130, *Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals*, (November 28, 2000), *available at* http://www.whitehouse.gov/omb/circulars_a130_a130trans4.

[73] With certain exceptions, a matching program is "any computerized comparison of -- (i) two or more automated systems of records or a system of records with non-federal records for the purpose of (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under federal benefit programs. . . ." 5 U.S.C. § 552a(a)(8)(A)(i)(I).

[74] The Secretary of Homeland Security is required to appoint the Chairperson and other members of the Data Integrity Board. 5 U.S.C. § 552a(u)(2). The Inspector General is a statutory member of the Data Integrity Board. 5 U.S.C. § 552a(u)(2).

[75] 5 U.S.C. § 552a(o).

Appendix D – Published PIAs and SORNs

Privacy Impact Assessments Published July 1, 2013 – June 30, 2014

Component	Name of System	Date Published
CBP	DHS/CBP/PIA-019 Air and Marine Operations Surveillance System (AMOSS)	7/22/2013
CBP	DHS/CBP/PIA-018 Aircraft Systems	9/18/2013
CBP	DHS/CBP/PIA-017 Non-Intrusive Inspection (NII) Systems Program	1/16/2014
CBP	DHS/CBP/PIA-006(c) Automated Targeting System (ATS) Common Operating Picture (COP)	1/31/2014
CBP	DHS/CBP/PIA-020 Export Information System (EIS)	1/31/2014
CBP	DHS/CBP/PIA-023 Biographic Visa and Immigration Information Sharing with Canada	2/10/2014
CBP	DHS/CBP/PIA-024(a) Arrival Departure Information System (ADIS)	3/5/2014
DHS-wide	DHS/ALL/PIA-046-1 Neptune Pilot	9/25/2013
DHS-wide	DHS/ALL/PIA-046-2 Common Entity Index Prototype	9/26/2013
DHS-wide	DHS/ALL/PIA-046 DHS Data Framework	11/6/2013
DHS-wide	DHS/ALL/PIA-046-3 Cerberus Pilot	11/22/2014
FEMA	DHS/FEMA/PIA-030 FEMA Smartphone Application with Disaster Reporter Feature	7/29/2013
FEMA	DHS/FEMA/PIA-031 Authentication and Provisioning Services (APS)	8/6/2013
FEMA	DHS/FEMA/PIA-020(a) Web Integrated Financial Management Information System Update	8/13/2013
FEMA	DHS/FEMA/PIA-032 Deployment Program	8/16/2013
FEMA	DHS/FEMA/PIA-033 Deployment Qualifications Program	8/16/2013
FEMA	DHS/FEMA/PIA-034 Electronic Fingerprint System	9/24/2013
FEMA	DHS/FEMA/PIA-035 Customer Satisfaction Analysis System	2/27/2014
FEMA	DHS/FEMA/PIA-036 Emergency Notification System (ENS)	4/7/2014
FEMA	DHS/FEMA/PIA-038(a) Virginia Systems Repository (VSR): Data Repositories	5/12/2014
FEMA	DHS/FEMA/PIA-037 National Responder Support Camp (NRSC)	5/28/2014
ICE	DHS/ICE/PIA-037 Electronic Health Records (eHR) System	7/24/2013
ICE	DHS/ICE/PIA-017(a) ICE Child Exploitation Tracking System (CETS)	8/28/2013
ICE	DHS/ICE/PIA-032(a) - FALCON Search and Analysis System	1/16/2014

Component	Name of System	Date Published
ICE	DHS/ICE/PIA-038 FALCON Data Analysis and Research for Trade Transparency System	1/16/2014
ICE	DHS/ICE/PIA-003 Electronic Travel Document (eTD)	2/6/2014
ICE	DHS/ICE/PIA-015(f) - Enforcement Integrated Database (EID) Update	4/8/2014
NPPD	DHS/NPPD/FPS/PIA-010(b) FPS Dispatch Incident Records Management System Update	3/25/2014
NPPD	DHS/NPPD/PIA-018(a) Chemical Facilities Anti-Terrorism Standards Personnel Surety	5/1/2014
OPS	DHS/OPS/PIA-008(c) HSIN Release 3 User Accounts: Identity Provider within the National Information Exchange Federation	2/18/2014
S&T	DHS/S&T/PIA-008(c) Facial Recognition Data Collection Project Update	9/16/2013
S&T	DHS/S&T/PIA-028 Air Entry/Exit Re-engineering (AEER) Project	5/28/2014
S&T	DHS/S&T/PIA-027 Test Data	6/23/2014
TSA	DHS/TSA/PIA-014(a) Crew Member Self Defense Training Program	7/24/2013
TSA	DHS/TSA /PIA-018(f) Secure Flight Program Update	9/4/2013
TSA	DHS/TSA /PIA-041 TSA Pre√™ Application Program	9/4/2013
TSA	DHS/TSA/PIA-034(a) – TSA Enterprise Performance Management Platform (EPMP)	3/3/2014
TSA	DHS/TSA/PIA-042 TSA OIA Technology Infrastructure Modernization Program	3/26/2014
TSA	DHS/TSA/PIA-043 Travel Protocol Office Program	3/26/2014
TSA	DHS/TSA/PIA-044 Vetting of Security Personnel Receiving International TSA Training Assistance	5/7/2014
USCIS	DHS/USCIS/PIA-047 GeoSpace	7/12/2013
USCIS	DHS/USCIS/PIA-048 USCIS International Visa Project	7/22/2013
USCIS	DHS/USCIS/PIA-019(b) Customer Relationship Interface System (CRIS)	8/15/2013
USCIS	DHS/USCIS/PIA-049 Refugee Access Verification Unit (RAVU)	8/16/2013
USCIS	DHS/USCIS/PIA-050 Standard Management Analysis Reporting Tool (SMART)	8/27/2013
USCIS	DHS/USCIS/PIA-030(b) E-Verify Self Check – Case Resolution Lookup	9/6/2013
USCIS	DHS/USCIS/PIA-003(a) Integrated Digitization Document Management Program (IDDMP)	9/24/2013
USCIS	DHS/USCIS/PIA-015(b) Computer Linked Application Information Management System 4	11/5/2013
USCIS	DHS/USCIS/PIA-024(a) Electronic Filing System (e-	12/30/2013

Component	Name of System	Date Published
	Filing)	
USCIS	DHS/USCIS/PIA-040 CasePro	2/3/2014
USCIS	DHS/USCIS/PIA-046 Customer Scheduling and Services	3/25/2014
USCIS	DHS/USCIS/PIA-044 Validation Instrument for Business Enterprise (VIBE)	4/15/2014
USCIS	DHS/USCIS/PIA-045(a) Deferred Action for Childhood Arrivals (DACA)	4/17/2014
USSS	DHS/USSS/PIA-012 USSS Credential Distribution System (CreDS)	7/11/2013
USSS	DHS/USSS/PIA-014 Field Support System (FSS)	9/18/2013

System of Records Notices Completed July 1, 2013 – June 30, 2014

Component	Name of System	Date Published
CBP	DHS/CBP-019 - Air and Marine Operations Surveillance System (AMOSS)	9/18/2013
DHS-wide	DHS/ALL-035 Common Entity Index Prototype System of Records	8/23/2013
DHS-wide	DHS/ALL-036 Board for Correction of Military Records	10/2/2013
DHS-wide	DHS/ALL-001 Freedom of Information Act and Privacy Act Record System	2/4/2014
DHS-wide	DHS/ALL-020 Internal Affairs	4/28/2014
FEMA	DHS/FEMA-006 Citizen Corps Program	7/22/2013
FEMA	DHS/FEMA/GOVT-001 National Defense Executive Reserve	11/21/2013
FEMA	DHS/FEMA-001 National Emergency Family Registry and Locator	11/21/2013
FEMA	DHS/FEMA-009 Hazard Mitigation, Disaster Public Assistance, and Loan Programs	3/24/2014
FEMA	DHS/FEMA-003 National Flood Insurance Program Files System of Records	5/19/2014
FEMA	DHS/FEMA-002 Quality Assurance Recording System (QARS)	6/20/2014
NPPD	DHS/NPPD-002 Chemical Facility Anti-Terrorism Standards Personnel Surety Program	5/19/2014
TSA	DHS/TSA-019 Secure Flight Records	9/10/2013
TSA	DHS/TSA-021 Precheck Application Program	9/10/2013
TSA	DHS/TSA-001 Transportation Security Enforcement Record System (TSERS)	12/9/2013
USCG	DHS/USCG-024 United States Coast Guard Auxiliary Database (AUXDATA)	4/24/2014
USCIS	DHS/USCIS-011 E-Verify Program System of Records	7/22/2013
USCIS	DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records	11/21/2013
USCIS	DHS/USCIS-008 Refugee Access Verification Unit (RAVU)	11/25/2013

Appendix E – Public Speaking Engagements

During this reporting period, the Chief Privacy Officer and Privacy Office staff spoke on privacy and FOIA topics at the following events:

July 2013

- Privacy and Civil Liberties Compliance Review and Legal Issues Working Groups Roundtable Event, Arlington, Virginia
- United States-Canada Information Sharing Meeting, Ottawa, Canada
- Chief Information Officer Council Meeting, Washington, DC

September 2013

- Data Privacy and Integrity Advisory Committee Meeting, Washington, DC

October 2013

- American Society of Access Professionals Seminar, Washington, DC
- NPPD's Privacy Awareness Week, Arlington, Virginia
- The Lemelson Center for the Study of Invention and Innovation, Smithsonian National Museum of American History Symposium, Washington, DC

November 2013

- Electronic Privacy Information Center Privacy Coalition Meeting, Washington, DC

December 2013

- American Society of Access Professionals Symposium, Washington, DC
- [DHS] OGC Intelligence and National Security Law Conference, Washington, DC

January 2014

- Federal Aviation Administration Privacy Week Symposium, Washington, DC
- Data Privacy and Integrity Advisory Committee Meeting, Washington, DC

February 2014

- RSA Conference, "Watching the Watchers: The New Privacy Officers Inside the U.S. Government," San Francisco, California

March 2014

- IAPP Global Privacy Summit, "Protecting Privacy under the Cybersecurity Microscope" panel, Washington, DC
- Electronic Privacy Information Center Privacy Coalition Meeting, Washington, DC
- DHS Women's History Month Program, Washington, DC

May 2014

- DHS Privacy Office Decade of Excellence Celebration, Washington, DC
- Beyond the Border Executive Steering Committee Meeting, Washington, DC
- American Society of Access Professionals National Training Conference, Arlington, Virginia

June 2014

- DHS Privacy Office's Annual Privacy Workshop, Washington, DC
- Government Technology Research Alliance Council Meeting, Leesburg, Virginia
- Federal CIO Council Boot Camp, Washington, DC
- Conference Board of Canada, Ottawa, Ontario
- The White House Office of Science & Technology Policy and Georgetown University hosted a workshop, *Improving Government Performance in the Era of Big Data: Opportunities and Challenges for Federal Agencies*, Washington, DC

Appendix F – Congressional Testimony and Staff Briefings

Congressional Testimony

The Chief Privacy Officer testified at one hearing during the reporting period, and her written testimony can be found on the Privacy Office website at www.dhs.gov/privacy:

November 19, 2013: Written testimony of DHS Chief Privacy Officer Karen L. Neuman for a Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce for a hearing titled "Strengthening Government Oversight: Examining the Roles and Effectiveness of Oversight Positions Within the Federal Workforce."

Congressional Staff Briefings

The Chief Privacy Officer and Privacy Office staff provided briefings on the following topics to congressional staff:

July 2013

- Congressional Unmanned Systems Caucus: Update on DHS's use of Unmanned Aircraft Systems

September 2013

- Senate Homeland Security and Governmental Affairs Committee: DHS Data Framework

October 2013

- Senate Select Committee on Intelligence: DHS Data Framework

November 2013

- Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on the Federal Workforce: Oversight role of the Privacy Office
- Senate Select Committee on Intelligence and House and Senate Appropriations Committee: Common Entity Index and Cerberus
- Senate Homeland Security and Governmental Affairs Committee: Update on DHS's use of Unmanned Aircraft Systems

January 2014

- House Homeland Security Committee: Privacy issues, including the use of Unmanned Aircraft Systems
- Senate Homeland Security and Governmental Affairs Committee: Update on various privacy issues

March 2014

- Senate Homeland Security and Governmental Affairs: Update on the Privacy Office FY 2015 budget
- Senate Appropriations Committee: Privacy Office's FY 2015 Budget Request

May 2014

- Senate Appropriations Committee Staff: Update on DHS's use of Unmanned Aircraft Systems

June 2014

- Senate Judiciary Committee Majority Staff: Update on DHS's use of Unmanned Aircraft Systems

Appendix G – International Outreach

The Chief Privacy Officer and other senior Privacy Office staff met with numerous international officials and organizations, some on multiple occasions, on a variety of topics during the reporting period, including:

- Canada Office of Privacy Commissioner
- Citizenship and Immigration Canada
- Canada Border Services Agency
- Privy Council Office, Canada
- Treasury Board of Canada
- Conference Board of Canada
- European Commission
- European Union Members of Parliament
- French Ministry of Culture
- German Members of State Parliaments
- Irish Office of the Data Protection Commissioner
- Kosovo Member of Parliament
- Justice and Home Affairs Senior Officials Meeting
- Norwegian National Security Authority
- Polish Ministry of Administration and Digitization
- Public Safety Canada
- Slovak Republic Ministry of Finance
- Spanish Ministry of Justice
- Swedish Ministry of Justice