Department of Homeland Security

Privacy Office

2013 Report to Congress

November 2013

Homeland Security

Message from the Deputy Chief Privacy Officer

November 6, 2013

I am pleased to present the Department of Homeland Security Privacy Office's *2013 Annual Report to Congress*, highlighting the achievements of the Privacy Office for the period July 2012 - June 2013, during which time I served as the Acting Chief Privacy Officer.

The Privacy Office's mission is to protect the privacy of all individuals by embedding and enforcing privacy protections and transparency in all DHS activities.

This year, I had the honor and opportunity to work with a talented and incredibly dedicated team of privacy and disclosure professionals in both the DHS Privacy Office and the Component privacy and Freedom of Information Act offices. I am impressed by the ability of these professionals to successfully build and sustain a culture of privacy and transparency across the Department. The complexity of DHS operations, and the diversity of its missions, consistently propels the Office to develop innovative privacy and disclosure policies and processes.

The accomplishments of the past year—many the culmination of previous years of effort—clearly demonstrate that the DHS Privacy Office is the premier federal privacy office in the United States, creating privacy and disclosure policy best practices that can be adopted across the Federal Government while serving as models for others.

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

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

Please direct any inquiries about this report to the Privacy Office at 202-343-1717 or privacy@dhs.gov. This report and other information about the Privacy Office are available on our website, www.dhs.gov/privacy.

Sincerely,

Jonathan R. Cantor
Deputy Chief Privacy Officer
U.S. Department of Homeland Security

Executive Summary

The Privacy Office (Privacy Office or Office) is the first statutorily created privacy office in any federal agency, as set forth in Section 222 of the *Homeland Security Act* (Homeland Security Act), 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 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 (FOIA) 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 (FIPPs) 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, 2012, through June 30, 2013, catalogues the Privacy Office's continued success in safeguarding individual privacy while supporting the Department of Homeland Security (DHS or Department) mission.

The Office's Fiscal Year (FY) 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 FIPPs;
- **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 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

- Issued three key policy documents :
  - Directive 140-06, *Privacy Policy for Research Programs and Projects*: The first such principles to be enacted in the Federal Government, this policy requires that privacy protections be built into all research programs and projects undertaken by the Department; and,
  - Instruction 047-001, *Chief Privacy Officer Investigations*: This policy memorializes key procedures the Chief Privacy Officer follows in the conduct of privacy investigations.
  - *Updated Policy for DHS Application of FOIA Exemption 6 to DHS Personnel Information Contained within Agency Records,* issued June 2013, provides updated guidance to ensure the Department processes personnel information contained within agency records in a consistent manner.
- Provided leadership and privacy subject-matter expertise in DHS's ongoing evaluation of its information sharing with the Intelligence Community (IC).
- Leveraged the expertise of the Data Privacy and Integrity Advisory Committee (DPIAC). During the reporting period, the DPIAC held two public meetings and issued two public reports:
  - *DPIAC Recommendations Paper 2012-01*, November 7, 2012, sets forth recommendations for DHS to consider when evaluating the effectiveness of cybersecurity pilots, and for specific privacy protections DHS can consider when sharing information from a cybersecurity pilot with other agencies.
  - *DPIAC Recommendations Paper 2012-02*, November 7, 2012, sets forth recommendations for DHS to consider when determining whether the collection and use of a biometric is warranted, and recommends specific privacy protections for DHS to consider when using biometrics for identification purposes.

Goal 2: Advocacy

- Established the Privacy, Civil Rights, and Civil Liberties Working Group on Unmanned Aircraft Systems (UAS) to evaluate the privacy implications of using sensor-equipped aircraft—including UAS—to accomplish DHS missions, and develop guidance materials for their use.
- Hosted a series of public meetings in tandem with CRCL to inform privacy and civil liberties advocates of the Department's activities under *Executive Order 13636, Improving Critical Infrastructure Cybersecurity*, and *Presidential Policy Directive 21, Critical Infrastructure Security and Resilience*.
- Continued to implement the Joint Statement of Privacy Principles (Beyond the Border Privacy Principles) in Beyond the Border (BTB) initiatives since the issuance of the *Beyond*

the Border Declaration[2] by President Obama and Canadian Prime Minister Harper in February 2011, and the release of the *Beyond the Border Action Plan.*[3]

- Deployed a web-based system to facilitate online FOIA requests, reducing response time.
- 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 (ISA-IPC), 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 FOIA policy, as well as providing briefings to the Congress on privacy and FOIA-related matters upon request.

Goal 3: Compliance

- Approved 87 new or updated Privacy Impact Assessments (PIA) and 24 System of Records Notices (SORN), resulting in a Department-wide Federal Information Security Management Act (FISMA) privacy score of 87 percent for required IT system PIAs, and 98 percent for SORNs. These scores are higher than last year's scores of 82 percent for PIAs, and 95 percent for SORNs.
- Reviewed 241 intelligence products and 519 Intelligence Information Reports. The Privacy Office is required by Departmental policy to review these products to ensure that only the minimum amount of personally identifiable information (PII) necessary to the intelligence value of the product is included.
- Received 811 FOIA requests during the reporting period, and processed 746.
- Partnered with the National Protection and Programs Directorate (NPPD) to publish a PIA on Enhanced Cybersecurity Services (ECS), a voluntary information sharing program that assists the owners and operators of critical infrastructure in enhancing the protection of their systems from unauthorized access, exploitation, or data exfiltration.
- Published the first Federal Government PIA on the use of UAS. The Science and Technology Directorate (S&T) partnered with the State of Oklahoma on the Robotic Aircraft for Public Safety (RAPS) project to test and evaluate Small Unmanned Aircraft Systems (SUAS) for potential use by the first responder community and DHS operational components.

Goal 4: Oversight

- Conducted a comprehensive review of the Department's compliance with the Automated Targeting System (ATS) PIA and SORN, and the 2011 U.S. – EU Passenger Name Record (PNR) Agreement[4] in advance of the July 2013 Joint Review with the European Commission.
- Completed six Privacy Compliance Review (PCR) reports covering a range of programs including the Department's use of social media for situational awareness, the E-Verify Self Check Program's use of a third-party identity proofing service, and information sharing.

---

[2] http://www.whitehouse.gov/the-press-office/2011/02/04/declaration-president-obama-and-prime-minister-harper-canada-beyond-bord

[3] http://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf

[4] *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 (2011 PNR Agreement).

- Provided 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 Federal CIO Council Privacy Committee (Privacy Committee), and in public settings.
- 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 providing guidance to staff at the National Aeronautics and Space Administration and the Department of the Treasury.
- Based on the January 2012 PCR[5] of the EINSTEIN Program, NPPD developed and implemented a quarterly review process for PII handling associated with cyber incident reporting and information sharing to ensure that the handling of PII is consistent with five recommendations to improve privacy protections.

Goal 5: Workforce Excellence

- The Privacy Office continuously strives to balance available resources with the staffing levels needed to meet the Office's mission. During this reporting period, Privacy Office management focused on sustainable and efficient use of resources, such as expanding opportunities for in-house or no-fee training, minimizing reliance on contractor support, and deactivating underutilized wireless and network services.
- Facilitated professional development workshops for Office staff to provide practical insights and lessons learned on problem solving, communications, sustaining quality in the public sector, and other important skills.

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 principles of the American way of life.

[5] The PCR can be found here: http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_nppd_ein.pdf

Privacy Office

2013 Annual Report to Congress

Table of Contents

Legislative Language

This report has been prepared in accordance with the Homeland Security Act, which includes the following requirement:

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 Privacy Office's 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, 2012 through June 30, 2013, 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. In light of this symbiotic relationship between privacy and transparency, 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.[6]

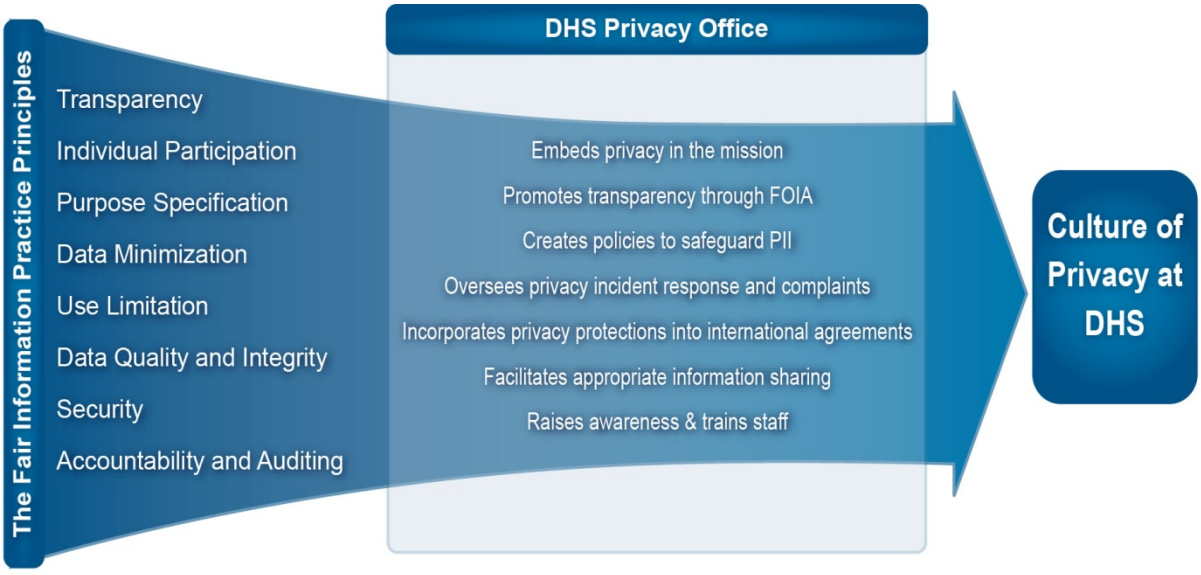


Figure 1: Privacy Office Implementation of the FIPPs

[6] 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.

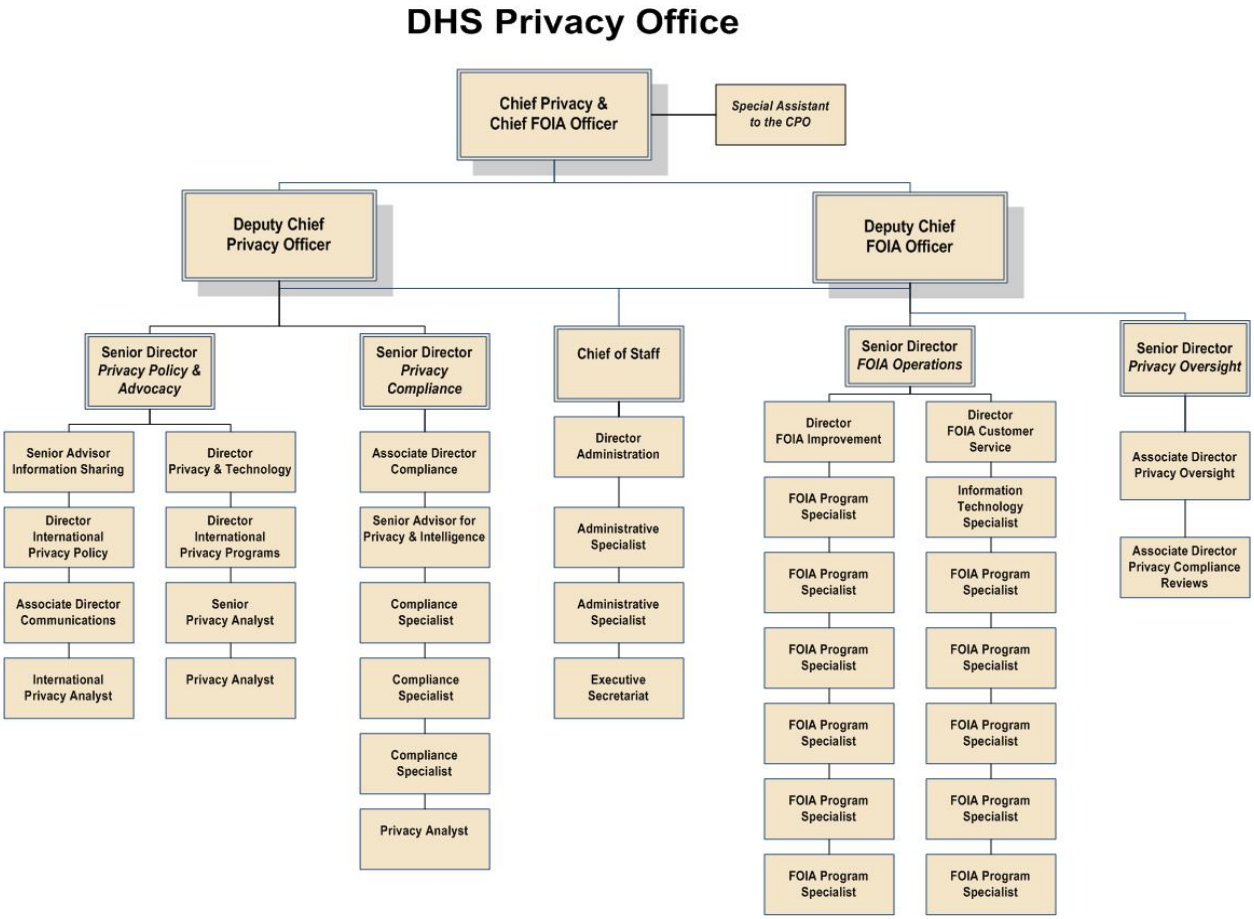
The Privacy Office incorporates these universally-recognized principles into privacy and disclosure policy and compliance processes throughout the Department. The Office also undertakes these statutory and policy-based responsibilities in collaboration with DHS Component privacy officers, privacy points of contact (PPOC),[7] 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 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



[7] 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, and international engagement. 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 performs coordination and oversight of 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 privacy incidents, and providing response and redress for 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

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.

Privacy Policy Directives and Instructions

The Privacy Office issued two important privacy policy documents during this reporting year:

1. Directive 140-06, *Privacy Policy for Research Programs and Projects*,[8] and its accompanying Instruction, "codify" a detailed set of privacy principles for privacy-sensitive research, the first such principles to be enacted in the Federal Government. The principles incorporate the FIPPs, and were informed by the consensus findings of participants in a public workshop on data mining convened by the Privacy Office in 2008[9]. The Directive requires that the principles be applied to all privacy-sensitive research, not just research that

[8] The Directive and its accompanying Instruction are available at http://www.dhs.gov/sites/default/files/publications/foia/privacy-policy-for-research-programs-and-projects-instruction-140-06-001.pdf

[9] More information on this public workshop can be found here: http://www.dhs.gov/privacy-workshops

involves data mining, and also requires that program staff work with Component privacy officers and the Privacy Office to develop implementation plans documenting how the principles are to be addressed in the research.

2. Instruction 047-01-001, *Chief Privacy Officer Investigations*, memorializes key procedures the Chief Privacy Officer follows in the conduct of privacy investigations.[10]

These two policy initiatives demonstrate the Department's ongoing commitment to furthering its mission in a manner that protects privacy.

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),[11] the Office for Civil Rights and Civil Liberties (CRCL), the DHS Office of Policy (PLCY), DHS Component data stewards, and external 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*,[12] the Privacy Office participated in the development of new Information Sharing Access Agreements (ISAA) with the National Counterterrorism Center[13] (NCTC). These ISAAs included new privacy protections related to transparency, oversight, and redress. As part of the DHS Records Working Group, the Privacy Office contributed to the development of a Data Retention Framework of Factors to determine appropriate periods for NCTC's retention of DHS datasets on a system-by-system basis. This framework includes factors related to operational considerations and the sensitivity of a dataset.
  - Through the Common Vetting Task Force (CVTF) and the DHS Records Working Group, the Privacy Office also participated in discussions with the Office of the Director of National Intelligence (ODNI) to discuss the privacy implications of sharing DHS information within the IC, since most DHS information is not collected under intelligence authorities and carries legal and policy considerations that may be different than the legal

[10] The Instruction is available at http://www.dhs.gov/sites/default/files/publications/foia/chief-privacy-%20officer-%20investigations-%20instruction-047-01-002.pdf

[11] 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.

[12] The Guidelines were approved in March 2012 and are available at: http://www.nctc.gov/docs/NCTC%20Guidelines.pdf.

[13] 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.

and policy considerations associated with intelligence information. For example, DHS missions do not regularly require DHS to distinguish between U.S. Persons and non-U.S. Persons, whereas this distinction is an integral aspect of intelligence oversight in the IC.

- 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 and 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 objectives related to enhanced privacy oversight of DHS's ISAAs.
  - As part of the DHS Records Working Group, the Privacy Office contributed to DHS directives on sharing information related to asylum seekers, asylees, and refugees. The Privacy Office also participates in a DHS working group to address Department responsibilities to protect Special Protected Classes of Aliens, as required by 8 U.S.C. § 1367.
  - As a member of the Office of Biometric Identity Management (OBIM), formerly known as United States Visitor and Immigrant Status Indicator Technology (US-VISIT),[14] Executive Steering Committee, the Privacy Office worked closely with OBIM to develop new processes for coordination with data owners to improve privacy and information sharing policy compliance.

  - The Acting Chief Privacy Officer serves as a member of the Homeland Security Information Network (HSIN) Executive Steering Committee, and partners with the 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. Through direct collaboration between the Privacy Office's policy and compliance experts and HSIN's strategy and design groups, DHS conducted two PIAs on HSIN Release 3's Identity Proofing Service in January 2013 and May 2013.
  - The Acting Chief Privacy Officer serves as a member of the 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 an enterprise level.

[14] In March 2013, the *Consolidated and Further Continuing Appropriations Act of 2013* the program's biometric identity management functions to OBIM, a newly created office within NPPD.

  - During this reporting period, the Acting Chief Privacy Officer, along with the Chief Information Officer (CIO) and the General Counsel, served on the Executive Steering Committee for Information Governance. The Acting Chief Privacy Officer provided governance, oversight, guidance, and approval across the Department for information governance to ensure the successful development, operation, and coordination of investments. The Acting Chief Privacy Officer also advised on strategic improvement opportunities, including the use of technology to improve the Department's FOIA processing; identified deficiencies and gaps; and made recommendations to facilitate collaboration among the stakeholders in the areas of records management, FOIA, privacy, and legal.
  - A new International Governance Board (IGB) was established during the reporting period, chaired by the Assistant Secretary for International Affairs, and charged with collaborating on the Department's International Engagement Plan. As an *ex officio* member, the Privacy Office ensures that the International Engagement Plan includes privacy compliance as a condition of all the new international information sharing initiatives included in the Plan.
- Provided information sharing policy leadership in DHS's internal information sharing and aggregation activities.
  - In coordination with the CIO, the Privacy Office co-chaired the DHS Data Aggregation Governance Working Group and contributed heavily to the development of the DHS Data Aggregation Governance Framework.
  - Through the CVTF, the Privacy Office collaborated on the development of requirements for projects related to data aggregation and the replication of unclassified DHS datasets to classified networks for use by DHS personnel working on classified networks, including the development of data tags and policy-based access controls to provide increased privacy protections.
- 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. This review included ISAAs with international, federal, state, local, territorial, and tribal partners.
  - Aside from its review of ISAAs for their compatibility with applicable privacy documentation, the Privacy Office also reviews for 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

Section 511(a) of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[15] (9/11 Commission Act) requires CRCL and the Privacy Office to provide training on privacy, civil rights, and civil liberties to all DHS officers and intelligence analysts before they deploy to state and major urban area fusion centers (fusion centers) and to support the training of all fusion center personnel nationwide on these same issues. CRCL and the Office have partnered with the I&A State and Local Program Office—the office within I&A that is the focal point for DHS support for fusion centers nationwide—and the Department of Justice's (DOJ) Bureau of Justice Assistance to develop and deliver this training program.

[15] 42 U.S.C. § 2000ee-1(f).

- Privacy Office staff provided the following training this year:
  - Trained 285 staff at seven fusion centers in collaboration with CRCL to complement the comprehensive, state-specific training delivered by each fusion center's privacy officials. The seven centers included: Maine, Georgia, Idaho, New Mexico, Southern Nevada, West Virginia and Utah;
  - Trained 82 analysts on privacy issues related to suspicious activity reporting; and,
  - Participated in the National Fusion Center Conference for the sixth consecutive year. Privacy Office staff trained 113 people on a variety of privacy topics, including intelligence product reviews and PIAs.

- During the reporting year, the Privacy Officer reviewed the Mariana Regional Fusion Center privacy policy and determined that it was "at least as comprehensive as the Information Sharing Environment (ISE) Privacy Guidelines." This brings the total number of approved State and Major Urban Area fusion centers privacy policies to 78.

Disclosure and Transparency Policy Initiatives

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

Proper Use of "Still-Interested" Letters in Compliance with Guidance from the Department of Justice (DOJ), Office of Information Policy, issued October 2012, directs DHS staff to adhere to the DOJ, Office of Information Policy (OIP) guidance dated March 4, 2010,[16] on strictly limiting the use of "still interested" letters or phone calls. The memorandum reminds staff that proper communication with the requester is paramount, and states that on occasion, the passage of time or a change in circumstance may give rise to a question of whether a FOIA requester is still interested in obtaining the requested records.

Updated Policy for DHS Application of FOIA Exemption 6 to DHS Personnel Information Contained within Agency Records, issued June 2013, provides updated guidance to ensure the Department processes personnel information contained within agency records in a consistent manner. The memorandum asserts that federal employees generally have no expectation of privacy regarding their names, titles, grades, salaries, bonuses, position descriptions, and duty stations, and as such, this information is generally releasable under the FOIA.[17] The memorandum *provides three c*ommon situations, however, in which the Department is likely to withhold the PII of certain DHS personnel on a case-by-case basis.

[16] U.S. Department of Justice, Office of Information Policy, FOIA Post, "OIP Guidance: The Importance of Good Communication with FOIA Requesters," March 4, 2010, http://www.justice.gov/oip/foiapost/2010foiapost5.htm
[17] 5 C.F.R. § 293.311.

Data Privacy and Integrity Advisory Committee

The DHS Data Privacy and Integrity Advisory Committee (DPIAC) provides advice 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, as well as data integrity and other privacy-related matters.[18]

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

- On July 17, 2012, the Committee received briefings on DHS's use of social media for situational awareness, including operations and oversight, and privacy protections embedded in the United States Coast Guard's (USCG) maritime biometrics programs.
- On November 7, 2012, DHS provided the Committee with an overview of the Department's cybersecurity activities. Committee members then discussed two separate draft subcommittee reports on cybersecurity pilots and the Department's use of biometrics. These reports were finalized and posted on the DPIAC website:

    - *DPIAC Recommendations Paper 2012-01*, November 7, 2012, sets forth recommendations for DHS to consider when evaluating the effectiveness of cybersecurity pilots, and for specific privacy protections DHS can consider when sharing information from a cybersecurity pilot with other agencies.
    - *DPIAC Recommendations Paper 2012-02*, November 7, 2012, sets forth recommendations for DHS to consider when determining whether the collection and use of a biometric is warranted, and recommends specific privacy protections for DHS to consider when using biometrics for identification purposes.

On April 29, 2013, the Secretary of Homeland Security appointed or reappointed ten members to the DPIAC.

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

[18] 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.

II. Advocacy

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.

Privacy Leadership and Collaboration within DHS

Within the Department, the Privacy Office's leadership and collaboration with the Components influences the scope and direction of programs that rely on personal information. The Office effectively partners with others to help evaluate and integrate privacy principles into Department activities.

- Established the Privacy, Civil Rights, and Civil Liberties Working Group on Unmanned Aircraft Systems (UAS) with CRCL, which the Privacy Office co-chairs with United States Customs and Border Protection (CBP) and CRCL. The Working Group provides 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 is completing 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. After publishing this document, the Working Group will continue to meet to determine if further guidance is needed to inform the Department's use of UAS;

- Developed new procedures and a new training curriculum for DHS Reports Officers, working with the Component members of the Reports Officer Management Council. The new curriculum covers the entire process of drafting Intelligence Information Reports (IIR), including Executive Order (EO) 12333 and how to incorporate privacy, civil rights, and civil liberties protections into IIRs;

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: *Executive Order 13636, Improving Critical Infrastructure Cybersecurity (EO-13636), and Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience.*[19] 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 and physical critical infrastructure in a manner that protects privacy and civil liberties. EO 13636 also 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.

EO 13636 also requires the Privacy Office and CRCL to compile assessments conducted by other departments and agencies into an annual report to be sent to the president initially in February 2014. The Privacy Office is working closely with DHS programs and Component privacy offices responsible for deliverables under EO 13636 to ensure that privacy protections are built into the planning and execution of related activities. The Privacy Office will begin its formal assessments of those activities in the next reporting year.

The Department established an Integrated Task Force (ITF) to lead DHS, interagency, and public and private sector efforts to implement EO 13636 and PPD-21.[20] The ITF is comprised of eight working groups, each focused on specific deliverables. The Privacy Office, together with CRCL, co-chairs the Assessments Working Group, an interagency forum for discussing issues related to privacy and civil liberties assessments required by EO 13636.

Additional information on DHS activities under EO 13636 and PPD-21 is included in Section VI of this report.

[19] 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.

[20] More information about the ITF is available on the DHS web site at http://www.dhs.gov/publication/integrated-task-force.

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[21] by President Obama and Canadian Prime Minister Harper in February 2011, and the release of the *Beyond the Border Action Plan*,[22] 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.

- **Training** – The Privacy Office developed flexible training materials and delivered Component-specific training on the BTB Privacy Principles to BTB action item leads at CBP, National Protection and Programs Directorate (NPPD), United States Immigration and Customs Enforcement (ICE), and the Office of the General Counsel (OGC). The Office continues to assess the need for additional or follow-up trainings.
- **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** – The Office participated in negotiations for the *U.S. - Canada Immigration Information Sharing Agreement*, signed in December 2012. Under the Agreement, biographic and biometric information will be exchanged on third-country nationals to assist in the administration and enforcement of U.S. and Canadian immigration laws, respectively. The Office assisted in the development of the implementing documentation for this Agreement, ensuring that privacy protections are appropriately incorporated in accordance with U.S. law, DHS policy, and the BTB Privacy Principles. Privacy compliance documentation will be established or updated as necessary before the Agreement is implemented.
  - **Entry/Exit Program** – The Office helped negotiate for the development 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. In addition to ongoing consultation and review of implementing documentation, privacy compliance documentation, such as PIAs and SORNS, has been developed and published for Phases I

[21] http://www.whitehouse.gov/the-press-office/2011/02/04/declaration-president-obama-and-prime-minister-harper-canada-beyond-bord
[22] http://www.dhs.gov/xlibrary/assets/wh/us-canada-btb-action-plan.pdf

and II. Further consultation and additional updates will be made as necessary for Phase III.

U.S. - EU Data Privacy and Protection Agreement. The Acting Chief Privacy Officer and 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 Five Country Conference*.** Privacy Office staff continued to support the PLCY-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. The Office negotiated an agreement with the United Kingdom on the sharing of visa, immigration, and nationality information, which was signed in April 2013.

Organization for Economic Cooperation and Development and Organization of American States. The Privacy Office continued to support interagency engagement with these two multilateral organizations, as each pursued high level privacy guidance that could potentially impact the DHS mission.

***Global Entry System*.** Privacy Office staff worked with CBP Privacy and the CBP Office of Field Operations on a template implementation arrangement for Global Entry System ISAAs to ensure inclusion of privacy protections in information sharing.

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.

Interagency Leadership

During the reporting period, the Office continued to play a role in the federal interagency community through active participation and leadership roles in key interagency fora and initiatives.

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 Staff and the Program Manager for the ISE at ODNI.

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. Additionally, the Privacy Office supports ISA-IPC efforts to implement the 2012 National Strategy for Information Sharing and

Safeguarding, 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 DHS Acting Chief Privacy Officer is a member of the standing Executive Committee of the ISA-IPC Privacy and Civil Liberties Subcommittee, the body that issues ISE Privacy Guidelines and manages their implementation. 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 requirements. This support includes:

- Technical assistance to support the development of ISE privacy policies;
- The development of draft guidance to streamline the process for developing information sharing agreements; and,
- The development and piloting of a compliance review self-assessment template.

The Federal CIO Council[23] Privacy Committee (Privacy Committee). The Acting DHS Chief Privacy Officer continued to serve as co-chair of the Federal CIO Council Privacy Committee, the principal interagency forum to improve federal agency practices for the protection of privacy. 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 laws and best practices advancing privacy. Privacy Office and Component privacy office staff supported the following subcommittees and Privacy Committee initiatives:

- **Best Practices Subcommittee** – Senior Privacy Office staff co-chair this Subcommittee. The Subcommittee collaborated with the National Institute for Standards and Technology (NIST) to implement the first ever appendix of privacy controls for NIST Special Publication 800-53, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations (Rev. 4) (SP 800-53)*. NIST released the final version of SP 800-53 Rev. 4 in April 2013.
- **Identity Management (IdM) Subcommittee** – Privacy Office staff co-chairs this Subcommittee. The IdM Subcommittee has been an active contributor this year to numerous Open Government initiatives and is particularly active in efforts relating to the ongoing development of the *Federal Identity, Credential and Access Management Roadmap and Implementation Guidance*. Currently the Subcommittee is compiling agency best practices to create a PIA for e-authentication programs.
- **Development and Education Subcommittee** – Privacy Office and NPPD Office of Privacy staff contributed to Subcommittee efforts to increase the number of privacy training opportunities for federal agency staff. The Subcommittee polled the SAOPs to determine their training needs, and then planned and delivered three formal training events, each to over

[23] The Federal CIO Council was first established by Executive Order 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/.

100 Federal Government employees and contractors. In addition, the Subcommittee conducted three informal sessions where privacy professionals gathered to share best practices on various topics.

- **Innovation and Emerging Technology Subcommittee** – With assistance from the Science and Technology Directorate's (S&T) Privacy Officer and NPPD Office of Privacy staff, this Subcommittee produced Deliverable 10.3 of the Federal CIO's Digital Government Strategy, which includes standardized controls for PIAs, PII inventories, and notice to individuals in the digital and mobile environment. The Subcommittee also updated its best privacy practices for the use of social media by federal agencies; developed additional terms of service (e.g., breach notification, compliance with Office of Management and Budget (OMB) Memorandum 10-23) for the General Services Administration to use when negotiating with social media service providers; and participated with the interagency cloud working group on developing privacy-related clauses for use in cloud contracts (i.e., data breach, PIAs).

Other Interagency Initiatives

- **National Science and Technology Council (NSTC),[24] Subcommittee on Privacy and Internet Policy, International Working Group** – Privacy Office staff regularly contributes 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. Privacy Office staff continues to contribute to the Working Group's development of United States Government responses to the proposed *European Union Data Protection Regulation and Directive*.[25]

- **NSTC Subcommittee on Biometrics and Identity Management** – Privacy Office staff regularly contributes to the work of the NSTC Subcommittee on Biometrics and Identity Management. The Subcommittee serves as an interagency forum for discussion of biometric and identity-related science and technology matters, and is a valuable resource for staying apprised of national efforts undertaken by the Federal Government related to biometrics and identity technology.

- **National Security Telecommunications Advisory Committee (NSTAC)[26] Nationwide Public Safety Broadband Network Subcommittee** – Privacy Office staff provides privacy subject-matter expertise to the NSTAC Nationwide Public Safety Broadband Network (NPSBN) Subcommittee, which is responsible for developing recommendations for the implementation of the NPSBN. The NPSBN will provide a secure, reliable, and dedicated interoperable network for emergency responders to communicate during an emergency.

[24] The NSTC was established by Executive Order 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.
http://www.whitehouse.gov/administration/eop/ostp/nstc

[25] In January 2012, the European Commission proposed a Regulation setting out a general European Union framework for data protection, entitled "*Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).*" That same month the European Commission proposed a Directive entitled "*Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.*"

[26] http://www.dhs.gov/nstac

Engaging the Public

Throughout this reporting period, the Privacy Office continued to actively promote awareness and robust public dialogue on vital privacy issues. The 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:

- **Redesigned Privacy Office website**: DHS completely overhauled its main website, www.dhs.gov, in August 2012, resulting in a new look with enhanced navigation and improved usability.
- **Privacy advocate meetings**: The Acting Chief Privacy Officer continued to host informational meetings with members of the advocacy community. He also updates the privacy advocacy community periodically by email and telephone conference calls about new privacy-related policies, reports, and activities.
- **EO 13636 Advocate Briefings:** To enhance transparency in advance of the first annual report, the Office and CRCL hosted a series of briefings on the Department's activities under EO 13636 for privacy and civil liberties advocates. Over the course of five bi-weekly sessions, interested advocates heard detailed briefings by leaders of each of the eight working groups.
- **Secretary's Blog on Cybersecurity:** The Office drafted a blog post, "Securing Cyberspace While Protecting Privacy and Civil Liberties," in which the Secretary outlined how EO 13636 clears the way for more efficient sharing of cyber threat information between the Federal Government and the private sector while also directing federal departments and agencies to incorporate robust privacy and civil liberties protections into all of their cybersecurity activities.
- **FOIA Requester Roundtables**: The Office hosted two open forum meetings with representatives from the Office of Government Information Services and several members of the requester community to discuss FOIA-related fees and fee waivers.
- **Speaking engagements**: The Acting Chief Privacy Officer and Privacy Office staff spoke on privacy topics at 25 events during this reporting period. See Appendix E for a detailed list of these engagements.

DHS Privacy and Transparency Training

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

Highlights from this reporting period include:

- **Updated mandatory annual privacy training:** In March 2013, this course was enhanced to include a segment on information sharing with law enforcement.
- **FOIA issues training**: The Privacy Office hosted a series of topical trainings on evolving FOIA issues:
  - In October 2012, DOJ's OIP hosted a workshop on new FOIA Exclusions Guidance;
  - In December 2012, OIP provided instruction on FOIA fees and fee waivers; and,

  - In May 2013, OIP trained the Department's FOIA staff, as well as staff from the Office of the Chief Procurement Officer, on FOIA Exemption 4 and contracts.

- **FOIA training for Office of Health Affairs, IGA, and DHS Operations Security Working Group staff:** In September 2012, February 2013, and June 2013, the Privacy Office provided the staff with a FOIA overview.
- **Annual Privacy Compliance Workshop**: In June 2013, 180 personnel from 45 federal agencies attended the Privacy Office Annual Privacy Compliance Workshop. This annual one day workshop provides in-depth training on DHS privacy compliance processes and best practices.
- **"DHS 201" International Attaché Training:** The Department's "DHS 201" training module is a weeklong course designed to prepare DHS employees who take on new roles as DHS attachés at U.S. embassies worldwide by providing them with basic information on each Component's international activities. The Privacy Office participates in each training session and provides an international privacy policy module to raise awareness among new attachés of the potential impact of global privacy policies, and to inform them of DHS privacy policy along with resources to support their overseas objectives. The Office conducted five training sessions during the reporting period.
- **Privacy training for Office of the Chief Financial Officer (CFO) staff**: The Privacy Office trained CFO staff on best practices for safeguarding PII.
- **Reports Officer training certification course**: The Office helped create and deliver a new training certification program for officers who prepare intelligence reports.
- **Compliance training boot camp**: The Privacy Office Compliance Team instituted two intensive eight-week compliance boot camp training programs for new compliance analysts and privacy analysts within the Department. The program is repeated when new privacy staff on-board. At each session, trainees practice using the FIPPs to mitigate privacy risk, and learn privacy compliance documentation requirements.

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.

- ***2012 Annual FOIA Report to the Attorney General of the United States* (February 2013)**:[27] 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.
- ***2013 Chief Freedom of Information Act Officer Report to the Attorney General of the United States* (March 2013)**:[28] 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.
- ***2012 DHS Data Mining Report to Congress* (February 2013)**: This report describes DHS activities already deployed or under development that fall within the *Federal Agency Data Mining Reporting Act of 2007* [29] definition of data mining.

The Acting 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.

[27] http://www.dhs.gov/sites/default/files/publications/foia/privacy-foia-annual-report-fy-2012-dhs_0.pdf
[28] http://www.dhs.gov/sites/default/files/publications/privacy/Reports/Final%20DHS%202013-chief-foia-officer-report-final_0.pdf
[29] 42 U.S.C. § 2000ee-3.

III. Compliance

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 integrate both privacy and FOIA compliance 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.

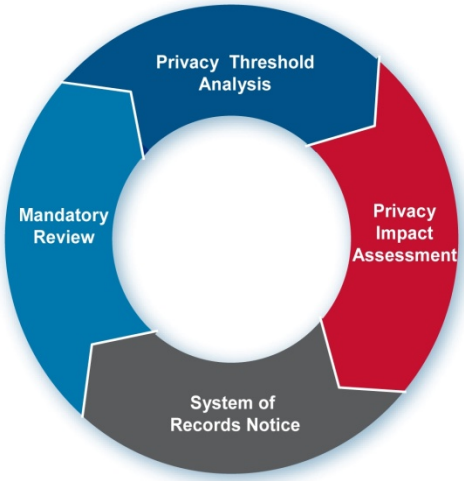


Figure 3: Privacy Office Compliance Process

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)[30] privacy reporting. The Office also conducts privacy reviews of 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:

- At the end of June 2012, the Department's FISMA privacy score showed that 82 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 95 percent of required SORNs had been completed. As of June 2013, the Department has improved this score to 87 percent of PIAs for required FISMA-related systems, and 98 percent of SORNs.[31]
- During the reporting period, the Department approved eight Computer Matching Agreements (CMA). 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. Additional information on CMAs is included in Appendix C.
- Reviewed 95 Information Technology (IT) investments for compliance with privacy requirements as part of the annual OMB 300 budget review process. The Privacy Office failed nine programs for lack of privacy compliance documentation. The Privacy Office has

[30] 44 U.S.C. § 3544.

[31] DHS must submit its privacy score under FISMA to OMB quarterly and annually. The privacy score is based on the number of IT systems that are marked privacy sensitive and require a PIA and/or SORN as compared to the total number for which documentation has been approved. Accordingly, these statistics are not static as new systems come online and old systems are retired.

actively worked with these programs to bring them into compliance and anticipates that several will pass during the review process that began in June 2013.

- Reviewed and approved 19 Social Media Operational Use Templates (SMOUT)[32] during the reporting period. In June 2012, the Department issued Management Directive 110-01, *Privacy Policy for Operational Use of Social Media*, which requires all DHS Components to submit a SMOUT to the DHS Privacy Office for review. For the purposes of the Management Directive and the SMOUT, "operational use" means the authorized use of social media to collect PII for the purpose of enhancing situational awareness, investigating an individual in a criminal, civil, or administrative context, making a benefit determination about a person, making a personnel determination about a Department employee, making a suitability determination about a prospective Department employee, or for any other official purposes that have the potential to affect the rights, privileges, or benefits of an individual.
- In partnership with CRCL and OGC, the Office conducted quarterly reviews of CBP's and the Transportation Security Administration's (TSA) 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, and published an updated PIA for the ATS program.

The Department's Federal Information Security Management Act (FISMA) privacy score improved this year.

As of June 2013, the Department had a FISMA score of 87 percent for PIAs for required FISMA-related IT systems, and 98 percent for SORNs.

[32] SMOUTs are used to document the process to be followed by all programs engaging in operational uses of social media; to identify information technology systems, technologies, rulemakings, programs, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer; and to assess whether there is a need for additional privacy compliance documentation.

The Privacy Office publishes new and updated PIAs on its website at www.dhs.gov/privacy. During the reporting period, the Acting Chief Privacy Officer approved 87 new or updated PIAs. Figure 4 illustrates the number of approved PIAs completed by Component during this reporting period.[33]

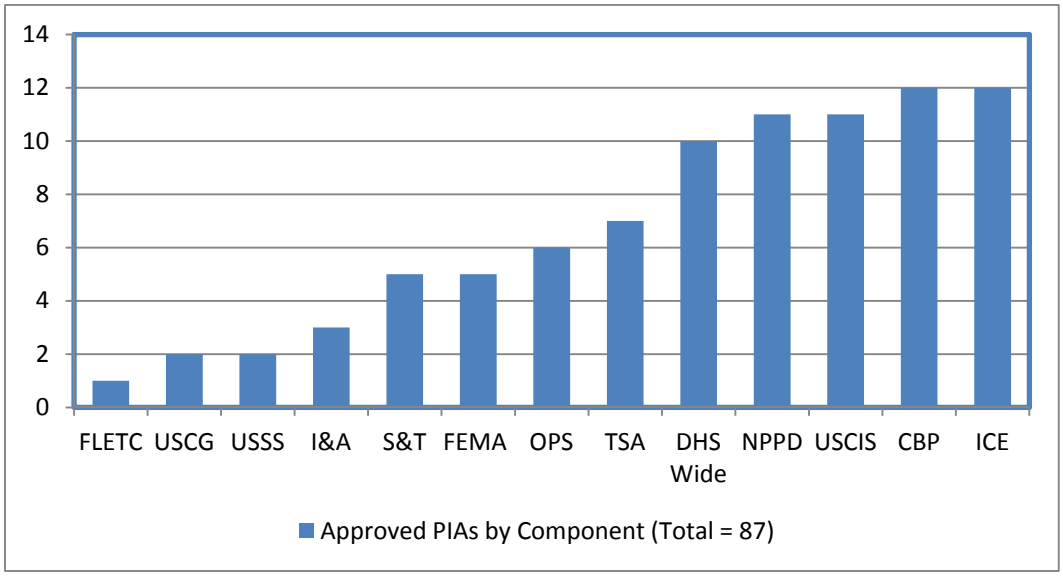


Figure 4: Number of Approved PIAs by Component During the Reporting Period

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

- ***DHS/NPPD/USVISIT/PIA-002 – Automated Biometric Identification System (IDENT)***
  Background: IDENT is the central DHS-wide system for storage and processing of biometric and associated biographic information for national security; law enforcement; immigration and border management; intelligence; background investigations for national security positions and certain positions of public trust; and associated testing, training, management reporting, planning and analysis, or other administrative uses.
  Purpose: This PIA provides transparency on how the system uses PII and describes the system's sharing partners and functions. *(December 7, 2012)*

[33] This represents the total number of new or updated PIAs that were approved by the Acting 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, 2013, will be included in the Privacy Office 2014 Annual Report, and made available at www.dhs.gov/privacy.

- ***DHS/NPPD/PIA-028 – Enhanced Cybersecurity Services (ECS)***
  Background: ECS is a voluntary program based on the sharing of indicators of malicious cyber activity between DHS and participating Commercial Service Providers. The purpose of the program is to assist the owners and operators of critical infrastructure in enhancing the protection of their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program. ECS consists of the operational processes and security oversight required to share unclassified and classified cyber threat indicators with companies that provide internet, network, and communication services to enable those companies to enhance their services to protect U.S. Critical Infrastructure entities. ECS is intended to support U.S. Critical Infrastructure; however, pending deployment of EINSTEIN intrusion prevention capabilities, ECS may also be used to provide equivalent protection to participating federal civilian Executive Branch agencies.
  Purpose: NPPD conducted this PIA because PII may be collected. This PIA consolidates and serves as a replacement to the DHS/NPPD/PIA-021 National Cyber Security Division Joint Cybersecurity Services Pilot PIA, published on January 13, 2012, and the DHS/NPPD/PIA-021(a) National Cyber Security Division Joint Cybersecurity Services Program, Defense Industrial Base – Enhanced Cybersecurity Services PIA Update, published on July 18, 2012. *(January 16, 2013)*

- ***DHS/NPPD/PIA-027 EINSTEIN 3 Accelerated (E^3A)***
  Background: DHS's Office of Cybersecurity and Communications (CS&C) continues to improve its ability to defend federal civilian Executive Branch agency networks from cyber threats. Similar to EINSTEIN 1 and EINSTEIN 2, DHS deployed EINSTEIN 3 Accelerated (E^3A) to enhance cybersecurity analysis, situational awareness, and security response. With E^3A, DHS can detect malicious traffic targeting Federal Government networks and also prevent malicious traffic from harming those networks. This is accomplished by delivering intrusion prevention capabilities as a Managed Security Service provided by Internet Service Providers (ISP). Under the direction of DHS, ISPs will administer intrusion prevention and threat-based decision-making on network traffic entering and leaving participating federal civilian Executive Branch agency networks.
  Purpose: DHS conducted this PIA because E^3A analyzes federal network traffic, which may contain PII. *(April 19, 2013)*

- ***DHS/OPS/PIA-008(b) - HSIN Release 3 (R3) User Accounts: Identity Proofing Service***
  Background: HSIN is maintained by OPS. HSIN facilitates the secure integration and interoperability of information sharing resources among federal, state, local, tribal, private-sector, commercial, and other non-governmental stakeholders involved in identifying and preventing terrorism, as well as in undertaking incident management activities. The HSIN program prepared this PIA Update to clarify information about HSIN's use of, and the data handling practices of, the identity proofing service (IDP Service).
  Purpose: This PIA documents the program's updated understanding of the information collected and stored by the IDP Service during, and following, new user registration on the HSIN R3 platform. *(May 22, 2013)*

- ***DHS/CBP/PIA-014 Centralized Area Video Surveillance System***
  Background: The Centralized Area Video Surveillance System (CAVSS), a system of cameras and separate microphones recording video and audio, respectively, furthers CBP's mission by collecting and maintaining video images and audio recordings of persons involved in any incidents or disturbances while seeking entry or admission into the United States, including secondary inspections.
  Purpose: CBP conducted this PIA because CAVSS uses information technology to collect, maintain, and disseminate PII in the form of video and audio recordings. *(May 24, 2013)*

During this reporting period, the Acting Chief Privacy Officer approved and published 24 SORNs, which are listed by Component in Appendix D. Figure 5 illustrates the number of SORNs completed by Component during this reporting period.

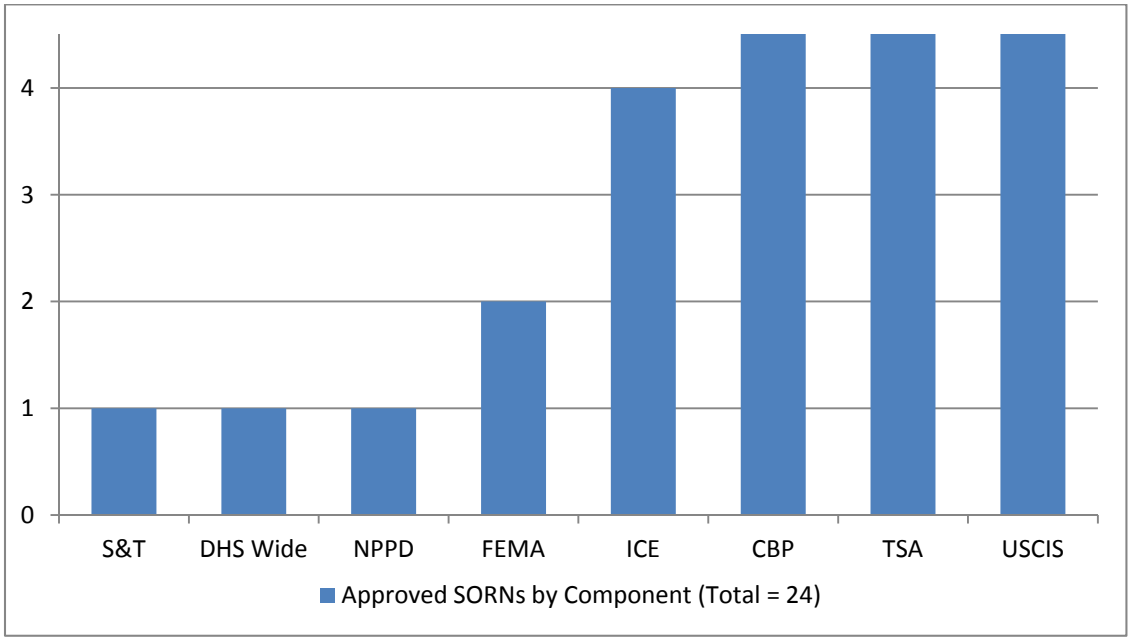


Figure 5: Number of Approved SORNs by Component During the Reporting Period

Intelligence Product Reviews

The Privacy Office reviews I&A classified and unclassified briefings, products, reports, directives, and other materials for privacy-related issues, and for compliance with privacy laws and regulations before release to the intelligence community and state and local stakeholders. 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 approximately 241 intelligence products and 519 IIRs.[34] The Office clears approximately 80 percent of all IIRs and products on first review with only minimal correction. The Office's review of IIRs and intelligence products

[34] 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.

continues to strengthen the quality of the products. Further, improvements to the IIR and product clearance rates demonstrate an enhanced integration of privacy protections.

Privacy Office staff continues 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 also tackling direct dissemination of IIRs by DHS Components, and levels classification of DHS IIRs.

FOIA Compliance

- **FOIA requests:**[35] In FY 2012, the Department received an unprecedented number of FOIA requests—190,589 in total—an increase of nine percent from FY 2011's total of 175,656. DHS processed 205,895 requests—an increase of 41 percent from 145,631 in FY 2011. From July 1, 2012 – June 30, 2013, the Privacy Office received 811 requests and processed 746 requests. This is a 92 percent closure rate which is outstanding considering the Office increased production by consolidating much of FOIA processing at headquarters to the Privacy Office, thereby increasing the workload despite shrinking staff resources. Additionally, by reporting time, the FOIA team was working to close the remaining pending requests, which tend to be complex. The ten oldest cases, which is another indicator of excellence established by DOJ, are closed.

- **FOIA backlog reduction**: The Department successfully reduced its backlog by 33 percent this year despite another record-breaking year in the volume of requests received. DHS took several steps to reduce the FOIA backlog, including the implementation of Six Sigma[36] to streamline operations, and the deployment of student interns, contractors, and Privacy Office staff to the Components with the largest backlogs. As a standard practice, FOIA staff negotiates with requesters to narrow the scope where practicable. In addition, Office staff met with Component FOIA Officers and FOIA 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.

- **FOIA operations:**[37] The Privacy Office and several of the Component FOIA Offices deployed a new electronic monitoring, tracking, and redacting commercial off-the-shelf software solution to streamline the processing of requests and appeals under FOIA and the Privacy Act. Results of the new software implementation include: (1) increased productivity; (2) enhanced accuracy in reporting statistics, tracking cases, and ensuring data integrity; and (3) improved interoperability and standardization of the FOIA process across the Department. This year, the Office also created a new position, Director of FOIA Improvement, whose role is to increase proactive disclosures, address the backlog, conduct FOIA training, and recommend enhancements to FOIA operations.

[35] For efficiency, Departmental data reflects the reporting period used in the *FOIA Annual Report.*
[36] Six Sigma is a management philosophy that emphasizes setting extremely high objectives, collecting data, and analyzing results to a fine degree as a way to reduce defects in products and services.
[37] 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*.

- **Online FOIA:** In August 2012, the Privacy Office deployed a web-based system enabling FOIA requesters to submit FOIA requests using an online form, reducing response time. The Office also redesigned its website, www.dhs.gov/FOIA, to make it easier for the public to find documents posted online and to submit requests. To promote transparency, the Office enhanced its online FOIA Library to feature a large number of frequently requested records pertaining to high visibility topics and guidance.

IV. Oversight

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

The Privacy Oversight Team, created in February 2012, includes 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: Privacy Compliance Reviews (PCR), 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 six PCRs.

These PCRs covered a range of programs including the Department's use of social media for situational awareness (National Operations Center (NOC) Publicly Available Media Monitoring and Situational Awareness Initiative), the E-Verify Self Check Program's[38] use of a third-party identity proofing service, and information sharing. During this reporting period, four of the six PCRs completed involved information sharing issues. Specifically, these four PCRs included DHS participation in the Nationwide Suspicious Activity Reporting (ISE-SAR) Initiative,[39] DHS development of a classified, multi-agency, information sharing environment, the NOC Counterterrorism Desk Database,[40] and DHS implementation of the 2011 U.S. – EU Passenger Name Record Agreement (discussed below).[41]

In addition to six completed PCRs, the Privacy Office also 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, the Privacy Office moved this program from a bi-annual to an annual PCR schedule, with a self-certification process to be completed by the NOC between annual PCRs. The Privacy Office will include the results of this self-audit in its report on the next annual PCR, which will begin in the fall of 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 Privacy Committee and in public settings. In November 2012, the Privacy Oversight Team gave a presentation on auditing privacy policies along with the results of its DHS ISE-SAR Initiative PCR at a Privacy/Civil Rights and Civil Liberties workshop for State and Local Fusion Center Privacy Officers held in Nashville, Tennessee. A session on how to conduct PCRs was also included in the Privacy Office's Annual Compliance Workshop for federal employees. The Privacy Oversight Team is committed to assisting other agencies as they strengthen their privacy programs by including PCRs in their oversight toolkits.

In a process similar to a PCR, the Chief Privacy Officer, together with representatives of CRCL, OGC, and relevant program staff, conducted quarterly reviews of rules used in ATS, to assess

[38] The Privacy Office is planning to conduct similar reviews for other DHS programs that use a third-party for identity proofing. These reviews will extend into FY 2014. For information about E-Verify Self Check see: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_everifyselfcheck.pdf.

[39] For information about the DHS ISE-SAR Initiative, see http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-dhswide-sar-update-20101117.pdf.

[40] http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_ops_ncod_07302012.pdf

[41] The results of the PCRs for the NOC Publicly Available Media Monitoring and Situational Awareness Initiative and for DHS implementation of the 2011 U.S. – EU PNR Agreement are documented in publicly available reports available on www.dhs.gov/privacy.

whether privacy and civil liberties protections are adequate and consistently implemented. The Office, CRCL, and OGC also met quarterly with NCTC staff to discuss NCTC's performance under several information sharing agreements with DHS, to assess implementation of the privacy and civil liberties-related provisions in those agreements.

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

During this reporting period, the Privacy Office conducted a comprehensive review of the Department's compliance with the ATS PIA and SORN and 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 (2011 PNR Agreement), which entered into force in July 2012).

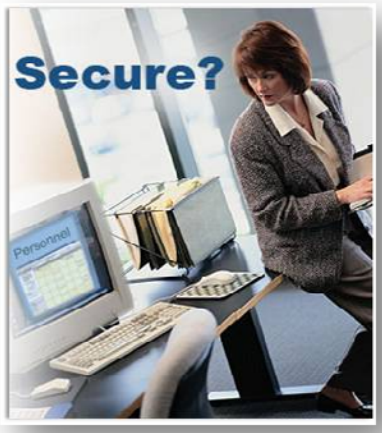
Article 23 of the 2011 PNR Agreement requires the parties to "jointly review the implementation of [the] Agreement one year after its entry into force" and on a regular basis thereafter. The Office's review, which began in April 2012 and culminated in a public report[42] published on July 3, 2013, found that with one minor exception, DHS fully complies with the 2011 PNR Agreement and with representations made in the PIA and SORN for ATS, the DHS system that maintains PNR. The report discusses areas of compliance and makes seven recommendations to improve compliance while ensuring the operational benefits of PNR remain intact. The Privacy Office report informed discussions during the 2013 Joint Review with the European Commission, which took place July 8 and 9, 2013, in Washington, DC.

[42] The report is available on the DHS Privacy Office website: http://www.dhs.gov/publication/dhs-pnr-privacy-review

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.[43] 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*.[44]

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. The Privacy Office is working with the Component's Privacy Officer to ensure that the Component documents new policies and operating procedures related to information sharing, and that the pilot, if continued, or any similar activity, is implemented in a privacy-protective manner.



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),[45] 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.

During this reporting period, 632 privacy incidents were reported to the DHS SOC, a decrease of eight percent from the last reporting period. The Department investigated, mitigated, and closed 534 (85 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.

[43] Congress expanded the authorities and responsibilities of the Chief Privacy Officer in 2007 in Section 802 of the 9/11 Commission Act, which added 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. 6 U.S.C. § 142.

[44] The Directive and its accompanying Instruction are available at http://www.dhs.gov/sites/default/files/publications/privacy/Directive_110-01_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf , and https://www.dhs.gov/xlibrary/assets/foia/Instruction_110-01-001_Privacy_Policy_for_Operational_Use_of_Social_Media.pdf, respectively.

[45] The PIHG is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.

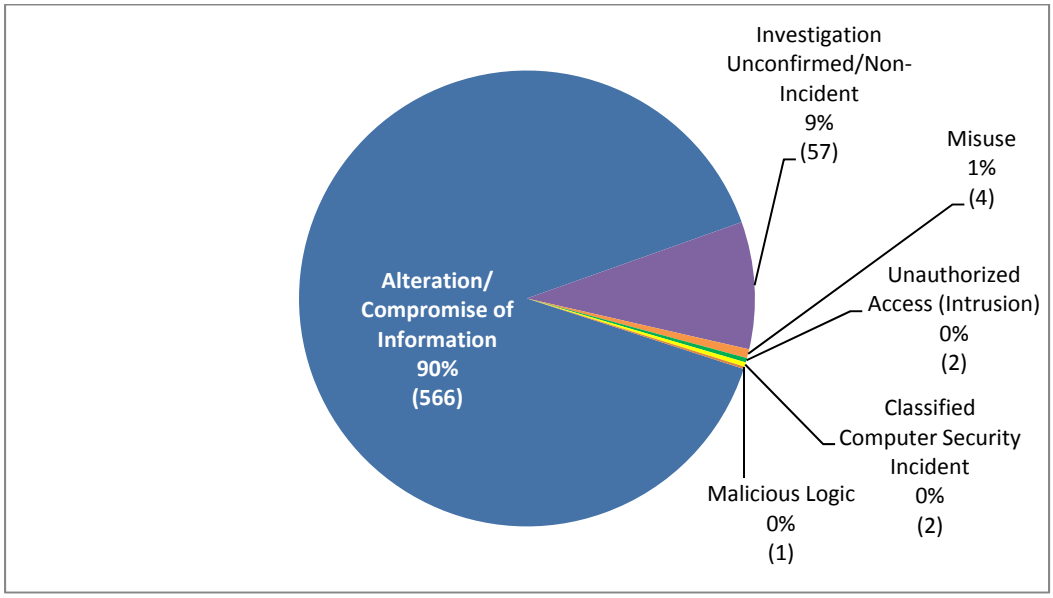


Figure 6: Percentage and Number of DHS Privacy Incidents by Type
July 1, 2012 - June 30, 2013 (total = 632)[46]

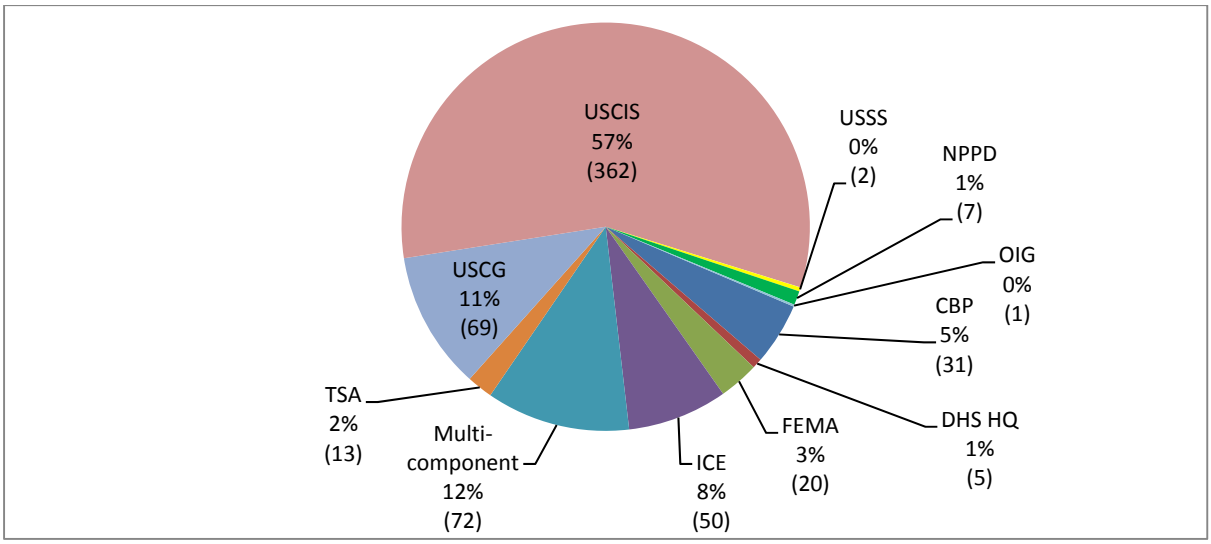


Figure 7: Percentage and Number of DHS Privacy Incidents by Component
July 1, 2012 - June 30, 2013 (total = 632)[47]

[46] 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/.
[47] "Multi-component" incidents are incidents that involve more than one DHS Component.

During this reporting period, the Privacy Office continued its efforts to reduce privacy incidents and to ensure proper incident handling procedures by having:

- Hosted the fourth annual DHS Core Management Group Meeting in September 2012, during which stakeholders met with the Acting Chief Privacy Officer to discuss privacy incidents and incident handling procedures;
- Held Privacy Incident Handling Quarterly Meetings in January and April 2013, 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 four site visits to DHS Components to discuss their privacy incident handling procedures and recommendations for improvement;
- Led sessions on privacy incident handling at two conferences for Federal Government personnel; and,
- Provided guidance on privacy incident handling to staff of the National Aeronautics and Space Administration and the Department of the Treasury.

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 allege that the Department has violated their privacy, or that the Department has not complied with privacy compliance requirements. U.S. citizens, Legal Permanent Residents, visitors to the United States, and aliens may submit privacy complaints to the Department.[48] 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, 2012, and May 31, 2013, the Department received 2,653 privacy complaints and closed 2,576.

Figure 8 shows the categories and disposition of privacy complaints the Department received between June 1, 2012 and May 31, 2013.[49]

Section 803 of the 9/11 Commission Act and OMB Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* [50] 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.

[48] The Department accepts complaints 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.

[49] The quarterly reporting period from June 2013 through August 2013 was ongoing at the close of the reporting period for this Annual Report. Statistics on privacy complaints submitted before June 2012 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.

[50] OMB Memorandum M08-21 is available at http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-21.pdf.

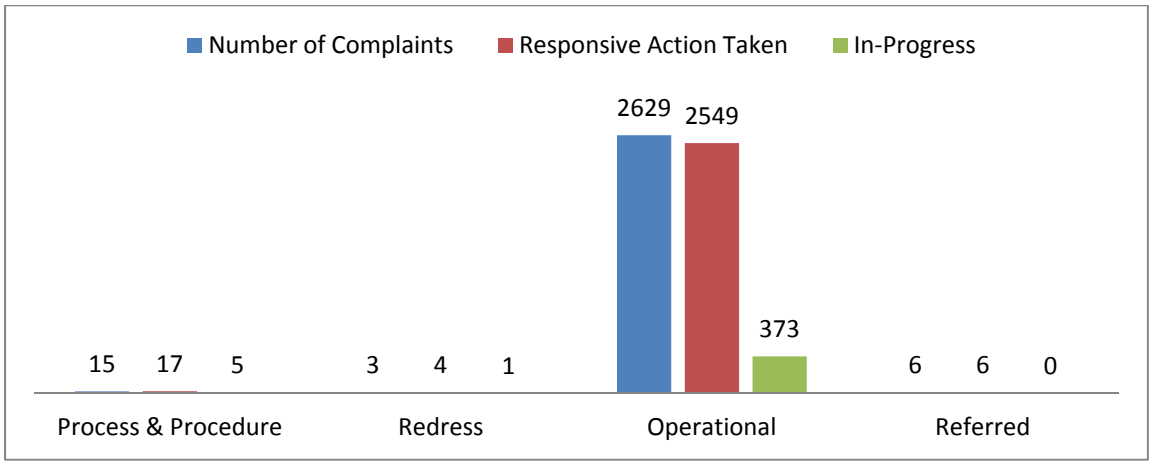


Figure 8: Privacy Complaints Received by DHS
June 1, 2012 – May 31, 2013[51]

Illustrative examples of privacy complaints submitted to the Department are included in the Privacy Office's Section 803 Reports.[52]

[51] 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.
[52] Available at http://www.dhs.gov/files/publications/editorial_0514.shtm.

Privacy Act Amendment Requests

Under Section (d)(2) of the Privacy Act, an individual may submit a request to the Department seeking amendment of his or her own records.[53] 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.[54] The Privacy Oversight Team serves as the repository for those statistics. During the reporting period the Office received no Privacy Act Amendment requests and DHS Components received 78 requests. Figure 9 shows Privacy Act Amendment Requests received by DHS during the reporting period by Component and disposition.

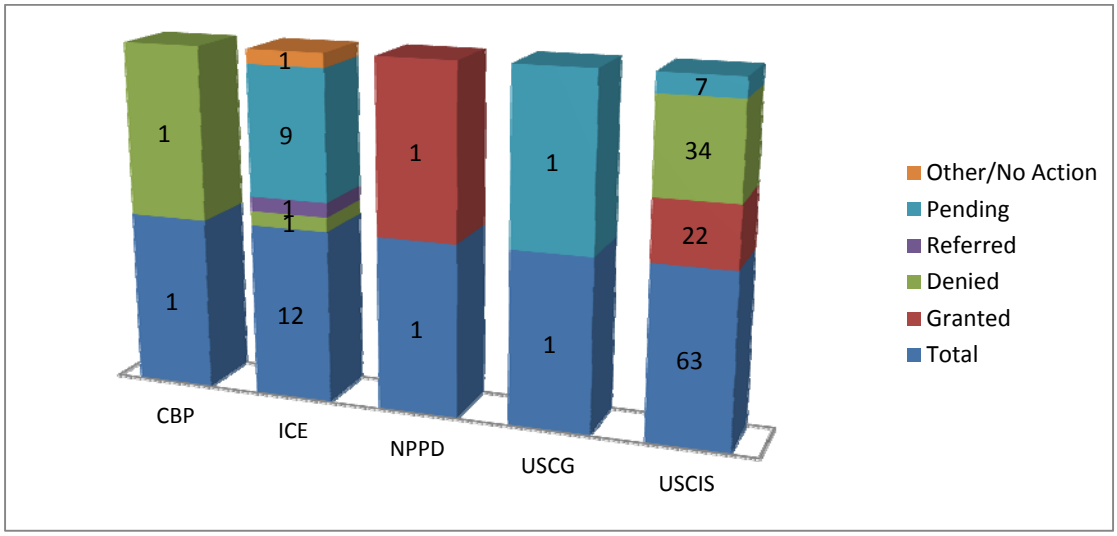


Figure 9: Privacy Act Amendment Requests by Component and Disposition
July 1, 2012 - June 30, 2013

[53] 5 U.S.C. § 552a (d)(2).
[54] http://www.dhs.gov/xlibrary/assets/privacy/privacy-policy-guidance-memorandum-2011-01.pdf

Non-Privacy Act Redress Programs

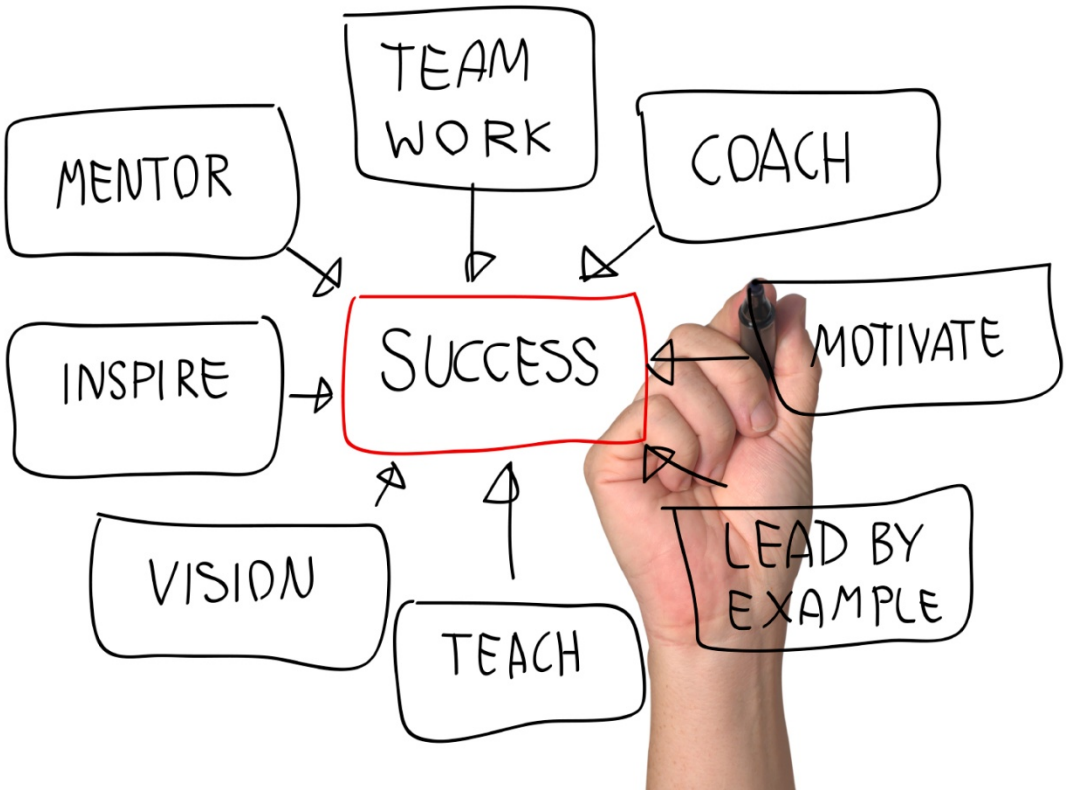
DHS also provides redress for individuals impacted by DHS programs through a number of other mechanisms, including:

- **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, 2012, through June 30, 2013, DHS TRIP received 17,731 requests for redress, with an average response time (from the time of first submission to final resolution) of approximately 33 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.

- **NPPD/Office of Biometrics Identity Management[55] (OBIM) Redress Program.** OBIM collects and maintains biometric information obtained 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 1,056 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 8,127 appeals and denied 373. Additionally, OLE/FAMS granted 2,514 waivers and denied 608.

[55] In March 2013, the *Consolidated and Further Continuing Appropriations Act of 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

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

The FY 2012-2015 Strategic Plan sets a high standard for the Office's workforce, aiming to "develop the best privacy and disclosure professionals in the Federal Government." This year, the Office worked diligently to make efficient use of its existing resources and maintain its leadership role in the federal privacy community through workforce development efforts.

Workforce Development Activities

During the reporting period, the Office conducted no-cost professional and leadership development workshops on a wide range of topics. In an effort to develop employee core competencies upon which all employees are rated annually, the Office coordinated panel discussions on customer service, and the skills required to represent the agency effectively. These workshops provided practical insights and lessons learned about problem solving, communication, sustaining quality in the public sector, and other important skills. DHS has a strong cadre of expertise among its workforce, and these self-initiated workshops represented an important means of tapping into that existing resource without incurring costs.

Keeping within the constraints of the current fiscal environment, the Office also encouraged its staff to take advantage of no-cost substantive classroom and online training offered by other DHS Components, as well as other government agencies.

To help grow a pool of talented privacy and transparency professionals, the Office aggressively recruited student interns from colleges and universities to assist with the efficient operation of the Office, and to make substantive contributions to its mission. In exchange, interns have gained deep insight into the Department's many important functions, and to the real-world application of FOIA, the Privacy Act, and other relevant statutes.

Office Efficiency and Sustainability

The Privacy Office has continued to work diligently to identify cost savings.

- As a headquarters staff office, personnel costs represent the largest proportion of the Privacy Office budget. Approximately 75% of the Office's enacted FY13 budget is allocated for salaries and benefits.
- 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, sufficient resources are not available to fill all existing vacancies within the Office.

During the reporting period, Office management focused on ways to cut costs and improve efficiency, such as expanding the use of in-house training, minimizing the use of contractor support, and deactivating underutilized wireless and network services. Similarly, the Office has taken steps to contribute to the Department's sustainability by reducing our physical footprint and costs associated with office space. The Office also acquired electronic cards that enable employees to use the public transportation system for local official travel, significantly reducing reliance on taxi fares and parking of personal vehicles. In addition, the Office took steps to reduce postage and mail processing costs to prevent waste and save public resources.

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 for 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

For the first time since its inception, the FEMA Privacy Officer and Deputy Privacy Officer deployed with other FEMA leadership in support of response and recovery operations during a disaster. This provided a unique opportunity to assess and make recommendations on enhancing privacy protections during disaster operations. Other significant activities during this reporting period included:

- Established privacy representation on FEMA's Strategic Leadership Steering Committee and Integrated Project Team for FEMA's agency-wide Workplace Transformation Initiative. Additionally, FEMA Privacy developed and disseminated privacy best practices fact sheets.
- Continued to serve on FEMA's Policy Working Group to ensure that all policies are developed to minimize privacy impacts. FEMA Privacy had the agency's Telework Policy revised to incorporate new requirements and procedures for safeguarding PII and other sensitive information while in use at alternate/telework sites. Additionally, FEMA Privacy developed and disseminated a FEMA-wide *Telework Best Practices Fact Sheet*.
- Developed and issued the first comprehensive FEMA Privacy Program Directive in May 2013, the first formal update to privacy direction at FEMA since 1987, based on the vision and objectives put in place by the new FEMA Privacy Officer.
- Created a FEMA Privacy Office Customer Service Manual, which details the suite of services provided by FEMA Privacy.
- Established 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, and Information System Security Managers to further the FEMA privacy mission.
- Established a new FEMA Privacy Office Disaster Operations Branch to address FEMA's disaster-related privacy issues and initiatives, and to implement the Office of Inspector General's (OIG) recommendations resulting from the FEMA Privacy Stewardship audit.

(See the Privacy Oversight section below for more details regarding the OIG's recommendations.)

Privacy Compliance

- Maintained a FISMA score for SORNs of 100 percent during this reporting period. The FEMA FISMA score for PIAs was 96 percent for this reporting period.
- Completed or updated 66 PTAs, 5 PIAs, and 2 SORNs during the reporting period.
- Continued and expanded the Privacy Compliance Surge[56] to update FEMA's inventory of privacy-sensitive systems. In doing so, FEMA addressed the privacy compliance of systems previously unidentified by the CIO, as well as FISMA systems, to ensure compliance with the privacy legal framework.
- Continued an information sharing initiative with the U.S. Small Business Administration (SBA) through a CMA to ensure 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 July 2014.

Privacy Incident Response and Mitigation

- Developed and distributed a comprehensive privacy incident remediation package to address incidents that require contract services to fulfill remediation efforts. This helped streamline FEMA's procurement process and create a more expeditious incident response and recovery process.

Privacy Training and Outreach

- Developed and disseminated a new factsheet, *How to Safeguard Sensitive PII*, and a new privacy poster, *Operationalizing Privacy*, to highlight methods of protecting PII and reporting privacy incidents.
- Developed and disseminated new privacy posters specific to disasters to highlight methods of protecting PII and reporting privacy incidents at disaster sites.
- Continued to conduct privacy awareness training for newly hired FEMA employees and contractors in the National Capital Region.
- Conducted specialized privacy awareness training for FEMA personnel in multiple locations.
- Hosted Privacy Compliance Foundations training for systems owners, program managers, Information System Security Officers, Information System Security Managers, and other

[56] FEMA's on-going effort, begun during the last reporting period, to establish privacy compliance around FEMA's inventory of privacy-sensitive systems.

personnel who handle or are responsible for ensuring that systems are in compliance with the privacy legal framework.

Privacy Oversight

On May 1, 2013, the OIG concluded its audit of FEMA's privacy stewardship and released a report with the following findings and recommendations:

1. Assess unauthorized systems and complete appropriate privacy compliance documentation;
2. Conduct privacy assessments of disaster relief operations;
3. Implement specialized privacy training for the disaster relief workforce; and,
4. Improve managers' capability to monitor and enforce employee and contractor compliance with the annual privacy awareness training requirement.

Before the conclusion of the audit, FEMA Privacy began implementing the OIG's recommendations. At the conclusion of this reporting period, three of the four OIG recommendations were closed. First, FEMA Privacy partnered with FEMA's CIO to assess the inventory of unauthorized systems using the established Privacy Office compliance process. FEMA Privacy also started building a framework to conducting privacy compliance site assessments at all FEMA locations, including disaster relief operations. In addition, FEMA Privacy began developing specialized training for the disaster relief workforce, and partnered with the FEMA CIO, Office of Chief Counsel, and Office of Response and Recovery to incorporate a more comprehensive compliance and accountability element into the annual privacy training module. OIG's final recommendation was to establish compliance around unauthorized systems, and this recommendation will be closed by the end of 2013.

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. In FY 2012, almost 70,000 students were trained, and, since it was established in 1970, approximately 1,000,000 law enforcement officers and agents have been trained at FLETC.

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

Privacy Policy Leadership and Development

- Recruited a new Information Access Officer for Privacy.
- Produced and published a privacy Frequently Asked Questions pamphlet.

Privacy Compliance

- Achieved a FISMA score of 100 percent for both PIAs and SORNs during the reporting period.
- Completed or updated 4 PTAs and 1 PIA during the reporting period.

Privacy Incident Response and Mitigation

- Collaborated on a recent DHS privacy incident to ensure that accurate and timely information and guidance was provided to impacted individuals.

Privacy Training and Outreach

- New Information Access Officer for Privacy met with department heads at FLETC to discuss general privacy issues and specific privacy concerns associated with their business practices.
- New Information Access Officer for Privacy attended the 2013 Privacy Compliance Workshop sponsored by the Privacy Office.

Privacy Oversight

- Staffed the FOIA & Privacy Program Office to ensure that FLETC is able to fulfill its privacy responsibilities.

National Protection and Programs Directorate (NPPD)

NPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. During this reporting period, the NPPD Office of Privacy (NPPD Privacy) supported the NPPD Office of the Under Secretary and the NPPD subcomponents, including the Federal Protective Service (FPS), OBIM, Office of Infrastructure Protection, and CS&C, and engaged in the following significant activities:

Privacy Policy Leadership and Development

- Assessed and established standards for surveys that are designed to gather opinions with the goal of improving service, soliciting feedback, or conducting research on behalf of NPPD, and developed a checklist to evaluate privacy and security considerations when administering surveys and using survey tools.
- Developed the Privacy Provisions for NPPD Solicitations and Statements of Work guidelines to identify core privacy provisions for compliance, required security and privacy training, and breach handling and notification. NPPD is now working to ensure that all acquired services comply with federal privacy requirements when contractors host or access government data that includes Sensitive PII.
- Partnered with the CRCL to develop an External Product Review Checklist outlining key privacy and civil liberties considerations that employees and contractors should be aware of when developing and reviewing external products. NPPD Privacy and CRCL presented the checklist and accompanying training to five separate offices within NPPD, and are currently working to develop a product review assessment process to evaluate the effectiveness of the checklist.
- Continued to chair the NPPD Social Media Working Group, working with the FPS, Office of Cybersecurity and Communications, and the Office of Compliance and Security to implement training and rules of behavior for the operational use of social media. In addition, the NPPD Office of Privacy worked with the NPPD Office of Public Affairs to develop standards for use of social media for communications and outreach with the public, as well as processes and procedures to govern access and use.

Privacy Compliance

- Maintained a 100 percent FISMA score for both PIAs and SORNs during this reporting period.
- Completed or updated 54 PTAs, 11 PIAs, and 1 SORN during the reporting period.
- Completed 10 Privacy Act statements as required by 5 USC 552a § (e)(3), 2 privacy notices, and 9 Paperwork Reduction Act packages.

Highlights of privacy compliance documents include:

- **OBIM published an update to the PIA on the Automated Biometric Identification System**. This is the DHS-wide system for storage and processing of biometric and associated biographic information. OBIM published the update to increase transparency for the system uses of PII and to detail its sharing partners and functions.
- **CS&C published the National Cybersecurity Protection System PIA**. This PIA evaluates the privacy impacts for DHS's intrusion detection, analysis, prevention, and information

sharing capabilities used to defend the Federal Civilian Government's IT infrastructure from cyber threats. This is a programmatic PIA that promotes transparency by providing a comprehensive understanding of the CS&C cybersecurity program to provide transparency.

Privacy Incident Response and Mitigation

Developed Standard Operating Procedures (SOP) for handling privacy incidents, consistent with the PIHG, that address roles and responsibilities as well as the procedures that must be followed in the event of a privacy incident. Although most incidents involve IT, a privacy incident may also involve physical security implications that may cause the compromise of PII; therefore this SOP applies to information in any format (e.g., paper, electronic).

Privacy Training and Outreach

During the reporting period, NPPD Privacy conducted training and awareness events:

- 1,428 NPPD personnel completed the online *DHS Culture of Privacy Awareness* course or its replacement course, *Privacy at DHS: Protecting Personal Information.*
- 1,401 personnel participated in instructor-led training, to include:
  - Privacy training at new employee orientation;
  - Role-based training for personnel in executive secretariat, personnel security, acquisitions, information assurance, and law enforcement positions; and,
  - Privacy awareness events and targeted privacy briefings.
- Partnered with CRCL to deliver a series of training sessions as part of the implementation of an External Product Review Checklist,[57] outlining key privacy and civil liberties considerations that employees and contractors should be aware of when developing and reviewing external products.
- Hosted a save-the-date event titled "*Got Cookies*?" to increase awareness of NPPD's Privacy Week events, and to educate employees about the privacy risks associated with web cookies. During this event, NPPD distributed new guidance, titled *Fact Sheet: Understanding Cookies*, as well as other privacy awareness materials.
- Held the second annual directorate-wide Privacy Week, October 22-26, 2012, to educate staff about how to protect personal information both at work and at home. The theme: "Privacy by Design: We Bake Privacy Protections into Everything We Do!" was weaved into every session, serving as a reminder that privacy should always be a core ingredient, not just a topping.
- Provided privacy briefings to each of the NPPD subcomponent Contracting Officers and Contracting Officer Technical Representatives to introduce new guidance on privacy provisions for NPPD solicitations and statements of work, as well as privacy tips for Contracting Officer Representatives.
- Released new guidance, titled "*How to Incorporate the Fair Information Practice Principles into Correspondence and Task Management*," geared toward the information management and executive secretariat community, and provided a directorate-wide briefing introducing the principles.

[57] The term "external product" refers to any reports, information bulletins, training, or other resource materials available to external audiences.

- Published four issues of the *Privacy Update*, NPPD's quarterly privacy awareness newsletter. Also, NPPD published privacy tips and trivia in the *US-VISIT Today* newsletter to highlight emerging privacy issues that impact the NPPD mission, as well as issues pertinent to employees' personal privacy.
- Issued privacy guidance to employees on a number of topics, such as safeguarding PII during office moves, protecting information from accidental disclosure, avoiding social engineering or phishing scams, and minimizing and protecting PII collected in connection with the Combined Federal Campaign.

NPPD Privacy also conducted these outreach activities:

- Helped organize the CIO Privacy Committee Development and Education Subcommittee's Safeguarding Sensitive PII training session, and served as a discussion leader for three informal meetings, during which NPPD shared best practices related to training human resources professionals on privacy, planning privacy awareness events, and responding to privacy incidents.
- Presented at the Library of Congress' National Data Privacy Day Seminar: *"Key Ingredients – Protecting Your Privacy Information."*
- Participated in a presentation titled "*The 411 on Cybersecurity, Information Sharing and Privacy*" at the International Association of Privacy Professionals (IAPP) Global Privacy Summit in Washington DC.
- Participated in the "One DHS Day on the Hill" event to provide awareness to Congressional Members and staff on matters relating to privacy and cybersecurity.
- Presented on PTAs at the annual DHS Privacy Compliance Workshop in Washington, DC.

Privacy Oversight

- Integrated privacy into the Information Technology Acquisition Review process to ensure that privacy is considered in the review of all IT acquisitions in excess of $2.5 million. NPPD Privacy reviewed over 40 Information Technology Acquisition Review packages since implementation of this process.
- Developed and implemented a quarterly review process for PII handling associated with cyber incident reporting and information sharing. This quarterly review ensures that the handling of PII is consistent with the five recommendations to improve privacy protections that came out of the January 2012 DHS Privacy Compliance Review for the EINSTEIN Program.
- Coordinated with the Privacy Office and CRCL to leverage oversight activities across the Department to implement EO 13636 and PPD-21, and to ensure that privacy, civil rights, and civil liberties are protected during all risk management efforts.

Office of Intelligence and Analysis (I&A)

I&A collects, analyzes, produces, and disseminates the intelligence information needed to keep the homeland safe, secure, and resilient. I&A provides intelligence support across the Department as well as to state, local, tribal, and territorial governments, and the private sector.

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

Privacy Policy Leadership and Development

- Created and maintained a privacy blog to explain the FIPPs and the requirements of the Privacy Act to I&A staff.
- Participated in a DHS working group to examine the privacy implications of expanded UAS use.
- Joined other privacy colleagues in developing processes and procedures to implement the President's cybersecurity initiative embodied in EO 13636 and PPD-21.
- Assisted the OIG in obtaining significant I&A participation in a privacy survey.
- Participated in the Watchlisting Cell Working Group to ensure that appropriate privacy protections are embedded in Department watchlisting activities.

Privacy Compliance

Through the efforts of the Privacy Officer, as well as training and outreach efforts, I&A personnel are well informed on the importance of privacy and intelligence oversight, and, as a result, they routinely come to the Privacy Officer for privacy policy guidance before developing, procuring, or revising IT systems.

- Completed or updated 19 PTAs and 3 PIAs during the reporting period, and began revisions on I&A's one SORN. [58]
- Worked with the I&A SharePoint team to ensure that all SharePoint sites are appropriately bannered when Sensitive PII is present and that other privacy requirements are met.
- Worked with Component privacy offices to perfect Privacy Act statements on forms.

Privacy Incident Response and Mitigation

- Helped mitigate the impact on Component employees of two data spills of varying severity. Both concerned the publication of DHS employee information on the Internet, but the data consisted of professional contact information (non-Sensitive PII) and employees were notified to be wary of phishing attempts.

Privacy Training and Outreach

- Provided Intelligence Oversight training, including privacy requirements, to all I&A staff, and separate privacy training to new I&A employees.
- Published frequent staff communications to raise awareness of privacy responsibilities, including the need to safeguard PII.

[58] I&A, as an element of the Intelligence Community, is exempt from FISMA reporting requirements.

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 Policy Leadership and Development

- Coordinated with CBP on the Secure Transit Corridors Pilot project to test a more secure and cost effective means of transporting goods across the U.S.-Mexico and U.S.-Canada land borders via truck or rail.
- Coordinated with several DHS Components on a project to test and evaluate small UAS. The test and evaluation program provides unbiased reports on small UAS capabilities for use in exigent circumstances where life or property are at risk, such as in building fires or during chemical spills.

Privacy Compliance

- Achieved a FISMA score of 100 percent for both PIAs and SORNs during this reporting period.
- Completed or updated 35 PTAs, 5 PIAs, and 1 SORN during the reporting period.
- Published the first Federal Government PIA on the use of UAS. S&T partnered with the State of Oklahoma on the Robotic Aircraft for Public Safety (RAPS) project to test and evaluate Small Unmanned Aircraft Systems (SUAS) for potential use by the first responder community and DHS operational components. SUAS include small aircraft that are operated using a wireless ground control station. The aircraft are equipped with sensors and cameras that can capture images and transmit them to a ground control system to provide aerial views of emergency situations and situational awareness. S&T conducted a PIA to address the privacy impacts of the system's surveillance and image capturing capabilities.

Privacy Incident Response and Mitigation

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

Privacy Training and Outreach

- Conducted privacy presentations on UAS at the IAPP Global Summit and at the Pre-Flight Briefing: *Public Safety Guidance on UAS Operations Conference*.
- Provided mandatory annual online privacy awareness training to all employees and contractors.

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 368 pending contract actions to implement PII handling and breach remediation requirements when necessary.
- Provided continuous advice and oversight on passenger screening protocols and security technology initiatives.
- Provided advice on risk-based screening proposals and TSA Pre✓™.

Privacy Compliance

- Increased its FISMA score for PIAs from 89 percent during the previous reporting period to 97 percent for this reporting period. Maintained a 100 percent FISMA score for SORNs during this reporting period.
- Completed or updated 49 PTAs, 7 PIAs and 5 SORNs during the reporting period.
- **Updates to the Credential Authentication Technology/Boarding Pass Scanning System**. This system validates the authenticity of passenger identity documents and/or boarding passes at TSA security checkpoints. TSA updated its PIA to reflect that it will network this system with the Secure Flight system in order to transmit passenger flight information to system devices at security checkpoints. The system will store the information for passengers at that airport for up to 24 hours after the scheduled flight time. The PIA update applies to those locations where TSA will pilot and deploy Secure Flight connectivity.

Privacy Incident Response and Mitigation

- TSA experienced one significant privacy incident during the reporting period when an employee improperly performed official work on a third person's non-DHS work laptop; the individual subsequently sent PII to several people after the relationship with the employee ended. The work laptop was promptly secured by the individual's employer, and recipients of the email were contacted to delete the PII. Credit monitoring was secured for potentially affected employees.
- The Privacy Office participated in testing of a Data Rights Management tool to investigate the operational potential for use by TSA to control access to sensitive information.

Privacy Training and Outreach

- Performed external outreach to a variety of privacy and civil liberties groups and thought leaders.
- Provided training to staff at TSA's Office of Intelligence & Analysis, the Office of Human Capital, Office of Law Enforcement/Personnel Security Division, and the Office of Information Technology/Information System Security Officers.

Privacy Oversight

- Incorporated privacy compliance elements in audit functions performed by the Management Control Oversight Program for internal controls at all TSA offices.
- Performed 40 annual program reviews to validate privacy documentation.

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, 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 memoranda:

- Memorandum (revised) on the use of Public Key Infrastructure (PKI) in the workplace to inform employees and contractors of the requirement to use PKI encryption software and to ensure that Sensitive PII collected and disseminated by USCIS personnel is protected both within and outside of the DHS firewall.
- Memorandum to inform employees and contractors of their responsibility to work with USCIS Privacy before starting or revising any initiative that involves the collection, use, or storage of PII, and the requirement to complete compliance documentation.
- Memorandum to inform employees and contractors of USCIS security requirements for maintaining PII and Sensitive PII on shared drives.
- Memorandum to inform employees and contractors of the requirement to complete annual privacy awareness training.
- Memorandum to inform USCIS employees and contractors of the privacy compliance process and the security requirements for maintaining Sensitive PII on Enterprise Collaboration Network (ECN) sites.

Privacy Compliance

- Increased its FISMA score for PIAs from 78 percent during the previous reporting period to 87 percent for this reporting period. Also increased its FISMA score for SORNs during this reporting period to 97 percent from 88 percent last year.
- Completed or updated 165 PTAs, 11 PIAs and 5 SORNs during the reporting period.

Highlights of privacy compliance documents include:

- **Published the Deferred Action for Childhood Arrivals PIA (DHS/USCIS-045)**. On June 15, 2012, the Secretary of Homeland Security issued a memorandum entitled, "*Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children*." The Secretary's memorandum sets forth how prosecutorial discretion may be exercised in cases involving certain people who arrived in the United States as children. The Secretary emphasized that generally, this population lacked the intent to violate the law, and that her memorandum would ensure enforcement resources would not be expended on these low priority cases. USCIS published this PIA because the Deferred Action for Childhood Arrivals process associated with this memorandum involves the collection and use of PII.

- **Published the Fraud Detection and National Security Directorate (FDNS) PIA (DHS/USCIS-044)**. FDNS is responsible for detecting, deterring, and combating immigration benefit fraud. USCIS conducted this PIA to document and assess how FDNS collects, uses, and maintains PII.

Privacy Incident Response and Mitigation

- Managed and mitigated 345 of the 362 reported privacy incidents involving a potential or actual compromise of PII. Mitigation is ongoing for the remaining 17 incidents.
- A significant incident occurred involving an unencrypted backup tape that was lost while in postal transit from the one field office to another. The lost PII included names, addresses, driver's license numbers, birth dates, and photos. To mitigate this incident, USCIS provided notification and credit monitoring to approximately 900 applicants. In addition, training was created that focused on incident management to ensure employees and contractors are aware of their responsibility to protect PII from unauthorized access, use, or disclosure, and reiterated reporting requirements. This training also provides guidance for identifying incidents; how to report an incident; when to report an incident; and procedures for informing appropriate staff of the incident.

Privacy Training and Outreach

- Launched a new mandatory online privacy training course: *USCIS Privacy Awareness Training* to convey privacy guidance specific to USCIS policy.
- Partnered with the USCIS Office of Security and Integrity, USCIS Record Management Branch, and USCIS Office of Chief Counsel to develop and broadcast a video on how to safeguard Sensitive but Unclassified (SBU) information.
- Partnered with the USCIS Records Management Branch to develop a privacy training that conveys best practices for safeguarding Sensitive PII and the USCIS process for reporting privacy incidents.
- 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.
- Created a compliance messaging strategy within the USCIS Western and Northeast Regions to communicate privacy issues to employees.

Trained the following:

- USCIS Research and Evaluations Division on Privacy Compliance, and how Division personnel should coordinate with USCIS Privacy on research projects that may involve PII.
- USCIS Headquarters (HQ) Field Operations Directorate and ECN facilitators on privacy requirements for sharing and storing Sensitive PII on ECN sites.
- USCIS HQ Field Operations Directorate and Refugee, Asylum and International Operations on privacy compliance requirements for the USCIS forms process.
- Northeast Region Office of Chief Counsel on how to disclose PII to third parties, and best practices for safeguarding PII.
- Mission Support Specialists on how to safeguard PII and respond to privacy incidents.

Privacy Oversight

- Implemented the USCIS Regional Privacy Officer Program to enhance and expand the USCIS privacy program. Program goals include: (1) promote a culture of privacy awareness with federal privacy laws, DHS regulations, and policies through education and awareness, training, and on site audits; (2) work collaboratively with the USCIS program and operational offices, along with the CIO, to ensure USCIS technology systems have appropriate privacy protections implemented according to privacy laws, regulations, and DHS policy; and (3) develop and distribute internal policy and guidance to promote, improve, and strengthen the operationalization of privacy processes according to privacy laws and regulations.
- Conducted and completed approximately 30 site visits and privacy risk assessments of various USCIS facilities, providing recommendations on ways to enhance privacy protections and increase awareness in each location.

United States Coast Guard (USCG)

For over two centuries, the USCG has safeguarded our nation's maritime interest in the heartland, in the ports, at sea, and around the globe. USCG protects the maritime economy and the environment, defends the maritime borders, and rescues those in peril at sea.

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

Privacy Policy Leadership and Development

- Collaborated with USCG Investigative Service and Intelligence directorates to establish Operational Use of Social Media "Rules of Behavior" for USCG law enforcement and intelligence element personnel.
- Updated policy prohibiting the release of USCG Employee Identification Numbers on the Internet.
- Partnered with the USCG PRA (Paperwork Reduction Act) Program Manager to promulgate an Information Collection Instruction policy.
- Partnered with DHS Components on the UAS Working Group to write the first draft of "*Protecting Privacy, Civil Rights and Civil Liberties Best Practices for UAS.*"
- Drafted white papers on data retention and data mining as a member of the DHS Big Data Working Group, comprised of numerous members from various federal agencies tasked to review, analyze, and submit a white paper on high level government issues (which included data retention and data mining) associated with "big data" collection.
- Participated as a member of the CIO Council Federal Privacy Committee's Innovation and Emerging Technology Subcommittee, comprised of privacy professional from across the Federal Government.

Privacy Compliance

- Maintained a FISMA score of 97 percent for PIAs and 100 percent for SORNs during this reporting period.
- Completed or updated 79 PTAs and 2 PIAs during the reporting period.

Highlights of privacy compliance documents include:

- **Published the Homeport Internet Portal PIA Update.** This PIA update included TSA Operations Center personnel as authorized users of Homeport's Alert Warning System, which will disseminate airport security information to authorized recipients. USCG uses the Homeport Internet Portal to provide secure information dissemination, advanced collaboration for Area Maritime Security Committees, complex electronic notification capabilities, and electronic submission and approval for facility security plans.
- **Published the Interagency Operations Center Watchkeeper PIA**. This system provides a fully functioning, shared operational picture for mission tasking and information response to all users within the Interagency Operations Center, to include local port and federal agency partners.

Privacy Incident Response and Mitigation

- As reported to the DHS SOC on December 3, 2012, security permissions on USCG home folders were improperly set, allowing files to be viewed by other USCG individuals without a need to know. The compromised files contained personnel evaluations as well as medical, legal, and law enforcement records, impacting over 10,000 USCG personnel. USCG secured the home folders and provided letters of notification along with one year of credit monitoring/identity counseling to the impacted individuals.

Privacy Training and Outreach

- Hosted two Privacy Awareness/Records Management fora in anticipation of the USCG's headquarters relocation. The fora emphasized privacy and records management best practices along with techniques for safeguarding Sensitive PII.
- Collaborated with the USCG HQ Command Security and Safety Office to co-sponsor the St. Elizabeth's Shred Initiative. USCG Privacy provided PII safeguarding guidance and monitored the event throughout USCG HQ to ensure compliance.

Privacy Oversight

- Presented the USCG Biometrics at Sea System briefing at the DPIAC meeting. USCG, NPPD's OBIM, Department of Defense, and DOJ are developing an Interim Support Plan to support the enhancement of border security through the USCG's use of mobile biometric devices to identify suspected individuals in the maritime milieu. USCG will utilize the Biometrics at Sea System to test the 10-print functionality in the Mona Pass and South Florida sectors.

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 an SOP for information sharing with law enforcement.
- 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.

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.
- Increased its FISMA score for PIAs from 22 percent during the previous reporting period to 38 percent for this reporting period. Also increased its FISMA score for SORNs during this reporting period to 84 percent from 77 percent last year.
- Completed or updated 31 PTAs, 12 PIAs and 5 SORNs during the reporting period.

Highlights of privacy compliance documents include:

- **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.
- **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.
- **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 the 31 CBP-only privacy incidents involving a potential or actual compromise of PII during the reporting period.
- CBP Privacy continues 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,[59] 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.

[59] 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

- Provided internal agency guidance on congressional disclosures pursuant to the Privacy Act.
- Issued five Social Media Operational Use Templates describing ICE's operational use of social media in the following areas: 1) criminal and administrative immigration law enforcement use; 2) criminal law enforcement use; 3) undercover criminal law enforcement use; 4) administrative law enforcement use; and 5) general non-law enforcement use.
- Issued Rules of Behavior for ICE's Operational Use of Social Media covering both (1) law enforcement uses (Use of Public and Non-Public Online Information); and (2) non-law enforcement uses (Use of Public Online Information for Non-Law Enforcement Work-Related Activities).

Privacy Compliance

- Increased its FISMA score for PIAs from 79 percent during the previous reporting period to 83 percent for this reporting period. The FISMA score for SORNs similarly increased from 98 percent to 100 percent for this reporting period.
- Completed or updated 45 PTAs, 12 PIAs and 4 SORNs during the reporting period.

Highlights of privacy compliance documents include:

- **Re-published the DHS/ICE-010 Confidential and Other Sources of Information SORN**. This SORN allows ICE to collect and maintain records concerning the identities of and information received from documented confidential informants and other sources who supply information to ICE regarding possible violations of law or in support of law enforcement investigations and activities. The SORN provides notice to the public regarding updates and changes to the system of records, including updates to the categories of individuals, the addition of new categories of records, updates to and the addition of new routine uses, and updates to the retention period of records.
- **Published a new PIA for the Visa Security Program Tracking System**. This case management system supports the ICE Visa Security Program. The system was upgraded from the original 2010 version to further modernize and automate the visa security screening process. The upgrade now allows ICE and CBP personnel to more effectively identify applicants for U.S. visas who are ineligible to enter the United States due to criminal history, terrorism associations, or other security-related grounds. ICE conducted this PIA because the upgrade changed the way that PII about individuals was collected, processed, and shared with other agencies.
- **Published a PIA, SORN, and an NPRM for the Imaged Documents and Exemplars Library.** This system is owned and operated by the ICE Homeland Security Investigation-Forensic Laboratory, an accredited crime laboratory 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 database and library contain two categories of records: (1) travel and identity documents and (2) reference materials used to help in the forensic analysis of travel and identity documents. The system contains electronic images and document characteristics for all documents, and reference materials stored in the library. The system allows laboratory employees to access these electronic images and document characteristics from their own workstations. ICE conducted this PIA because PII of individuals is often captured in the images and other records maintained in the system. The SORN provided notice to the public regarding the system's existence, and the NPRM 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.

Privacy Incident Response and Mitigation

- Ninety-two privacy incidents were reported and 84 were resolved. ICE Privacy was proactive to mitigate any damages from the incidents and help reduce the occurrence of future incidents.

Privacy Training and Outreach

- Conducted New-Hire Orientation privacy training sessions for approximately 220 ICE employees.
- Conducted 17 privacy training sessions for SharePoint collaboration site points of contact, training 38 ICE employees and contractors.
- Conducted two privacy training sessions for approximately 70 Office of the Principal Legal Advisor employees and contractors, addressing disclosures pursuant to the Privacy Act and privacy in general at ICE.
- Conducted one privacy training session for 25 Enforcement and Removal Operations and Office of State, Local, and Tribal Coordination employees and contractors, discussing general concepts in privacy and privacy at ICE.
- Conducted one privacy training session for 18 ICE Health Services Corps employees and contractors, discussing the safe handling of Sensitive PII and privacy incidents.
- Conducted two privacy training sessions for 25 Enforcement and Removal Operations Custody Programs and Community Outreach Training employees and contractors, discussing disclosures under the Privacy Act and privacy at ICE.
- Conducted one privacy training session for FOIA Office employees and contractors, discussing the relationship between FOIA and the Privacy Act and privacy at ICE.
- Presented at the FOIA Office Training, discussing privacy waivers and other disclosures under the Privacy Act, privacy violations and best practices, and ICE Privacy and Records Office responsibilities.

- Presented to the Homeland Security Investigations Fugitive Program Working Group, discussing disclosures under the Privacy Act.
- Presented at the DHS Core Management Group Meeting on the excellent relationship that ICE Privacy has fostered with the ICE Security Operations Center.

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' Information Technology Review Committee quarterly meetings to identify all newly proposed or operational systems, and facilitated engagement with project managers and program managers to ensure that privacy considerations were embedded in the design of each system.
- Established a Social Media Working Group to evaluate existing or planned uses of social media, and to ensure compliance with privacy requirements.
- Issued an official message to all employees and supervisors providing notification of a newly developed Secret Service privacy policy, which established rules of behavior for the use of social media for both law enforcement and non-law enforcement purposes.

Privacy Compliance

- Increased its FISMA score for PIAs from 71 percent during the previous reporting period to 88 percent for this reporting period, and increased its FISMA score for SORNs from 89 percent to 100 percent for this reporting period.
- Completed or updated 13 PTAs and 2 PIAs during the reporting period.
- Conducted a comprehensive review of USSS FISMA systems to identify systems requiring PTAs and PIAs.
- 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 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; and
- Staff responsibility to safeguard PII, Sensitive PII, and SBU when transmitted by email outside of USSS.

Privacy Training and Outreach

- Hosted a Privacy Awareness Day to convey privacy best practices.
- Posted privacy awareness posters and flyers to encourage staff to safeguard PII.
- Enhanced the USSS intranet page to disseminate information to employees about privacy compliance, guidelines, and tools. USSS also developed a Social Media Resources section on the intranet and posted all relevant policies and directives governing the use of social media by Secret Service employees for both operational and non-operational purposes.
- Provided mandatory online privacy awareness training to all Secret Service employees and contractors.
- Provided mandatory privacy training on the Operational Use of Social Media to employees whose positions require the use of social media for operational purposes.

The Future of Privacy at DHS

The Privacy Office has worked over the past nine years to create an environment in which privacy and security are not traded or balanced, but merged in a manner that keeps the country safe and honors the principles on which the country was founded. As a result, privacy is now firmly embedded into the lifecycle of DHS programs and systems to inform Departmental policy, and to ensure effective privacy protections. The full privacy compliance process provides the public with notice of what the Department does with personal information, and why.

While the DHS Chief Privacy Officer is responsible for privacy policy development at the Department, the Component privacy officers enhance the implementation of these policies because they are most familiar with the programs, offices, and systems that these policies affect, and where the potential privacy risks are. The Privacy Office will continue to nurture its relationship with these privacy professionals, providing them with guidance, resources, and training.

In the future, Americans will increasingly judge the success of DHS missions, programs, and activities in terms of how well the Department protects privacy and contributes to the greater understanding of privacy issues related to homeland security. To continue earning the trust and support of the public, the Department will need to understand how each of its activities impacts privacy and take affirmative steps both to protect privacy and to explain those protections to the public. DHS will need to develop new ways to think about privacy, and new methods of providing transparency to a more informed and skeptical public, even as resources tighten.

New homeland security threats will emerge, and technology—perhaps not yet imagined—will be part of the potential solution to those threats. This will require the Department to develop novel uses of data, cultivate new relationships, and deploy as yet unknown technologies. As a result, the demand for privacy professionals on the ground and at a strategic level will only increase, making the DHS Privacy Office and the Component privacy officers and privacy points of contact even more essential to the future of DHS.

As the Privacy Office enters its tenth year, it will continue to ensure that DHS stays committed to the FIPPs, protects the privacy of all individuals, and provides the greatest level of transparency possible.

Appendix A – Acronym List

Acronym List	
ATS	Automated Targeting System
BTB	Beyond the Border
CAVSS	Centralized Area Surveillance System
CBP	U.S. Customs and Border Protection
CFO	Chief Financial Officer
CIO	Chief Information Officer
CMA	Computer Matching Agreement
CRCL	Office for Civil Rights and Civil Liberties
CS&C	Office of Cybersecurity and Communications
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
ECN	Enterprise Collaboration Network
ECS	Enhanced Cybersecurity Services
EO	Executive Order
E^3A	EINSTEIN 3 Accelerated
FBI	Federal Bureau of Investigation
FDNS	Fraud Detection and National Security Directorate
FEMA	Federal Emergency Management Agency
FIPPs	Fair Information Practice Principles
FIR	Field Interview Report
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
HSIN	Homeland Security Information Network
HQ	Headquarters
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
IDENT	Automated Biometric Identification System
IDP	Identity Proofing Service
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
ISE-SAR	Information Sharing Environment-Suspicious Activity Reporting
ISP	Internet Service Provider
ISSGB	Information Sharing and Safeguarding Governance Board
IT	Information technology
ITF	Integrated Task Force
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
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NPSBN	Nationwide Public Safety Broadband Network
OBIM	Office of Biometrics Identity Management
OCIO	Office of the Chief Information Officer
ODNI	Office of the Director of National Intelligence
OGC	Office of the General Counsel
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	DHS Office of Operations Coordination and Planning
PACT	Privacy Administrative Coordination Team
PCR	Privacy Compliance Review
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIHG	Privacy Incident Handling Guidance
PLCY	Office of Policy
PKI	Public Key Infrastructure
PNR	Passenger Name Records
PPAT	Privacy Policy and Advocacy Team
PPD	Presidential Policy Directive
PPOC	Privacy Point of Contact
PRA	Paperwork Reduction Act
PTA	Privacy Threshold Analysis

Acronym List	
RAPS	Robotic Aircraft for Public Safety
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
SUAS	Small Unmanned Aircraft System
TSA	Transportation Security Administration
UAS	Unmanned Aircraft System
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:[60]

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.

[60] *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;[61]

(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.

[61] *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(a)(4) of the Homeland Security Act;
- **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.[62]

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.[63] The Chief Privacy Officer serves as the Chairperson of the DHS Data Integrity Board and members include the Inspector General and representatives of Components that currently have active CMA in place.[64]

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.[65]

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 even long-standing computer matching programs regularly.

[62] 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.

[63] With certain exceptions, a matching program is "any computerized comparison of two or more automated systems of records or a system of records with non-federal records for the purpose of 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).

[64] 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).

[65] 5 U.S.C. § 552a(o).

Appendix D – Published PIAs and SORNs

Privacy Impact Assessments Published July 1, 2012 – June 30, 2013

Component	Name of System	Date Published
DHS-wide	DHS/ALL/PIA-042 Closed Circuit TV	7/26/2012
DHS-wide	DHS/ALL/PIA-014(b) Personal Identity Verification (PIV) Update	8/23/2012
DHS-wide	DHS/ALL/PIA-002 - DHS Traveler Redress Inquiry Program (TRIP) (three-year checklist)	12/15/2012
DHS-wide	DHS/ALL/PIA-028(b) Department Freedom of Information Act and Privacy Act Records Program	2/13/2013
DHS-wide	DHS/ALL/PIA-012(b) E-mail Secure Gateway (EMSG)	2/28/2013
DHS-wide	DHS/ALL/PIA-006 DHS General Contacts Lists (Appendix Update)	3/19/2013
DHS-wide	DHS/ALL/PIA-043 Hiring and On-Boarding Process	4/23/2013
DHS-wide	DHS/ALL/PIA-042 Closed Circuit TV (Appendix Update)	5/17/2013
DHS-wide	DHS/ALL/PIA-002(a) - DHS Traveler Redress Inquiry Program (TRIP)	6/5/2013
DHS-wide	DHS/ALL/PIA-044 Single Point of Service (SPS) Request for Information (RFI) Tool	6/17/2013
FEMA	DHS/FEMA/PIA-025 – Hazard Mitigation Grant Program (HMGP) System[66]	7/31/2012
FEMA	DHS/FEMA/PIA-011 National Flood Insurance Program Information Technology System	10/12/2012
FEMA	DHS/FEMA/PIA-012(a) Disaster Assistance Improvement Program (DAIP)	11/16/2012
FEMA	DHS/FEMA/PIA-028 Mapping Information Platform	5/3/2013
FEMA	DHS/FEMA/PIA-009(a) - Document Management and Records Tracking System (DMARTS)	5/16/2013
FEMA	DHS/FEMA/PIA-029 Citizen Corps Program	6/28/2013
FLETC	DHS/FLETC/PIA-002-Student Administration and Scheduling System	2/13/2013
NPPD	DHS/NPPD/PIA-021(a) - Joint Cybersecurity Services Program (JCSP), Defense Industrial Base (DIB) – Enhanced Cybersecurity Services	7/18/2012
NPPD	DHS/NPPD/PIA-009 - Chemical Facility Anti-Terrorism Standards (CFATS)	7/26/2012
NPPD	DHS/NPPD/PIA-026 – National Cybersecurity	7/30/2012

[66] DHS/FEMA/PIA-025 – Hazard Mitigation Grant Program (HMGP) System PIA was approved on June 29, 2012, during the previous year's annual reporting period. However, the PIA published on July 31, 2012 and is therefore included in this year's Appendix of Published PIAs.

Component	Name of System	Date Published
	Protection System (NCPS)	
NPPD	DHS/NPPD/USVISIT/PIA-002 Automated Biometric Identification System - IDENT	12/7/2012
NPPD	DHS/NPPD/PIA-028 Enhanced Cybersecurity Services (ECS)	1/16/2013
NPPD	DHS/NPPD/USVISIT/PIA-002 Automated Biometric Identification System - IDENT: Appendix Update	3/4/2013
NPPD	DHS/NPPD/PIA-027 EINSTEIN 3 Accelerated	4/19/2013
NPPD	DHS/NPPD/USVISIT/PIA-002 Automated Biometric Identification System - IDENT: PCSC Taiwan Appendix	6/25/2013
NPPD	DHS/NPPD/USVISIT/PIA-002 Automated Biometric Identification System - IDENT: OBIM DHS-DOD IDENT Wrapback – Appendix Update	6/25/2013
NPPD	DHS/NPPD-001 EINSTEIN 1 (Three Year Checklist)	6/28/2013
NPPD	DHS/NPPD-008 EINSTEIN 2 (Three Year Checklist)	6/28/2013
OPS	DHS/OPS/PIA-007 HSIN 3.0 Shared Spaces On the Sensitive but Unclassified Network	7/25/2012
OPS	DHS/OPS/PIA-008 HSIN R3 User Accounts	7/25/2012
OPS	DHS/OPS/PIA-009 National Operations Center Operations Counterterrorism Desk (NCOD) Database	7/31/2012
OPS	DHS/OPS/PIA - 008(a) HSIN R3 Manual Identity Proofing Process	1/21/2013
OPS	DHS/OPS/PIA-004(d) Publicly Available Social Media Monitoring and Situational Awareness Initiative Update	4/1/2013
OPS	DHS/OPS/PIA-008(b) HSIN Release 3 User Accounts: Identity Proofing Service	5/23/2013
S&T	DHS/S&T/PIA-001(a) - Border Network and Northeast Test Bed (formerly BTSNet)	8/24/2012
S&T	DHS/S&T/PIA-024 Rapid DNA System	9/17/2012
S&T	DHS/S&T/PIA-025 Game Systems Forensics Development	10/11/2012
S&T	DHS/S&T/PIA-026 Robotic Aircraft for Public Safety (RAPS) Project	11/16/2012
S&T	DHS/S&T/PIA-008(b) Standoff Technology Integration and Demonstration Program: Biometric Optical Surveillance System Tests	12/19/2012
TSA	DHS/TSA/PIA-030(a) - Access to Sensitive Security Information in Contract Solicitations Update (SSI)	7/30/2012
TSA	DHS/TSA/PIA-037 - Automated Wait Time Technology (AWT)	8/5/2012
TSA	DHS/TSA/PIA-038 Performance and Results Information System	9/20/2012
TSA	DHS/TSA/PIA-039, Office of Intelligence & Analysis	11/15/2012

Component	Name of System	Date Published
	Trends and Patterns Branch (TPB)	
TSA	DHS/TSA/PIA-040, Port Authority of New York/New Jersey Secure Worker Access Consortium Vetting Services (SWAC)	11/15/2012
TSA	DHS/TSA/PIA-024(b) Credential Authentication Technology / Boarding Pass Scanning System	1/23/2013
TSA	DHS/TSA/PIA-004(b) Visitor Management System	3/13/2013
USCIS	DHS/USCIS/PIA-030(d) E-Verify Program Update	7/27/2012
USCIS	DHS/USCIS/PIA-006(a) Systematic Alien Verification for Entitlements (SAVE) Program	7/27/2012
USCIS	DHS/USCIS/PIA-044 Fraud Detection and National Security Directorate	7/30/2012
USCIS	DHS/USCIS/PIA-045 Deferred Action for Childhood Arrivals (DACA)	8/15/2012
USCIS	DHS/USCIS/PIA-036(a) Employment Eligibility Verification Requirements Under the Form I-9 Update	8/22/2012
USCIS	DHS/USCIS/PIA-038(a) FOIA/PA Information Processing System FOIA/PA Information Processing System (FIPS) Update	12/18/2012
USCIS	DHS/USCIS/PIA-006(b) Systematic Alien Verification for Entitlements (SAVE) Program Update	4/22/2013
USCIS	DHS/USCIS/PIA-030(c) E-Verify RIDE - Appendix Update	5/16/2013
USCIS	DHS/USCIS/PIA-027(b) Refugees, Asylum, and Parole System and the Asylum Pre-Screening System Update National Counterterrorism Center (NCTC)	6/5/2013
USCIS	DHS/USCIS/PIA-046 Customer Scheduling and Services (Infopass)	6/6/2013
USCIS	DHS/USCIS/PIA-036(b) Employment Eligibility Verification Requirements Under the Form I-9 Update	6/28/2013
USCG	DHS/USCG/PIA-001(b) Homeport Internet Portal Update	11/27/2012
USCG	DHS/USCG/PIA-020 InterAgency Operations Center (IOC) Watchkeeper	1/7/2013
USCG	DHS/USCG/PIA-019 Transportation Worker Identification Credential (TWIC) Reader Requirements[67]	3/25/2013
CBP	DHS/CBP/PIA-007(b) Electronic System for Travel Authorization (ESTA) Internet Protocol Address and System of Records Notice Update	7/18/2012
CBP	DHS/CBP/PIA-012 – CBP Portal (E3) to	7/27/2012

[67] DHS/USCG/PIA-019 Transportation Worker Identification Credential (TWIC) Reader Requirements PIA was approved on May 3, 2012, during the previous year's annual reporting period. However, the PIA published on March 25, 2013 and is therefore included in this year's Appendix of Published PIAs.

Component	Name of System	Date Published
	ENFORCE/IDENT	
CBP	DHS/CBP/PIA-004(f) - Western Hemisphere Travel Initiative: Beyond the Borders	9/28/2012
CBP	DHS/CBP/PIA-011 Intellectual Property Rights e-Recordation and Search Systems	1/15/2013
CBP	DHS/CBP/PIA-002(b) Global Enrollment System Update	1/16/2013
CBP	DHS/CBP/PIA-013 Customs Trade Partnership Against Terrorism (C-TPAT)	2/19/2013
CBP	DHS/CBP/PIA-016 I-94 Automation	3/1/2013
CBP	DHS/CBP/PIA-014 Centralized Area Video Surveillance System	5/24/2013
CBP	DHS/CBP/PIA-001(f) - Advanced Passenger Information System (APIS) Update National Counter Terrorism Center (NCTC)	6/5/2013
CBP	DHS/CBP/PIA-007(c) - Electronic System for Travel Authorization (ESTA) Update National Counter Terrorism Center (NCTC)	6/5/2013
CBP	DHS/CBP/PIA-004(g) - Beyond the Border Entry/Exit Program Phase II	6/28/2013
ICE	DHS/ICE/PIA-010(a) - National Child Victim Identification System (NCVIS)	7/26/2012
ICE	DHS/ICE/PIA-015(e) - Enforcement Integrated Database ENFORCE - EAGLE Update	7/26/2012
ICE	DHS/ICE/PIA-032(a) FALCON Search & Analysis System	11/2/2012
ICE	DHS/ICE/PIA-033 - FALCON Tipline (FALCON-TL)	11/5/2012
ICE	DHS/ICE/PIA-029 - ICE Alien Medical Records System	11/30/2012
ICE	DHS/ICE/PIA-020(d) Alien Criminal Response Information Management System (ACRIMe)	1/31/2013
ICE	DHS/ICE/PIA-008(a) Bonds Online System (eBONDS) Phase Two	1/31/2013
ICE	DHS/ICE/PIA-011(a) Visa Security Program Tracking System (VSPTS-Net) 2.0	1/22/2013
ICE	DHS/ICE/PIA-035 Imaged Documents and Exemplars Library	5/16/2013
ICE	DHS/ICE/PIA-032(a) FALCON Search & Analysis System (FALCON-SA) 2013 Appendix Update	6/3/2013
ICE	DHS/ICE/PIA-036 OPLA Case Management System	6/28/2013
USSS	DHS/USSS/PIA-011 - Cyber Awareness/Internet Threat Program (Cyveillance)	12/21/2012
USSS	DHS/USSS/PIA-013 CLEAR Clearance, Logistics, Employees, Applicants and Recruitment (CLEAR)	1/9/2013

System of Records Notices Completed July 1, 2012 – June 30, 2013

Component	Name of System	Date Published
DHS-wide	DHS/ALL-004 General Information Technology Access Account Records System	11/27/2012
FEMA	DHS/FEMA-008 Disaster Recovery Assistance Files	4/30/2013
FEMA	DHS/FEMA-009 Hazard Mitigation Assistance Grant Programs (HMAGP) System of Records	7/23/2012
NPPD	DHS/NPPD-VISIT-001 Arrival Departure Information System (ADIS)	5/28/2013
S&T	DHS/S&T-001 Research, Development, Test, and Evaluation Records	1/15/2013
TSA	DHS/TSA-019 Secure Flight Records	11/19/2012
TSA	DHS/TSA-009 General Legal Records System of Records	11/27/2012
TSA	DHS/TSA-012 Transportation Worker Identification Credential	11/27/2012
TSA	DHS/TSA-015 Registered Traveler (RT) Operations Files	11/27/2012
TSA	DHS/TSA-017 Secure Flight Test Records	11/27/2012
USCIS	DHS/USCIS-004 Systematic Alien Verification for Entitlements (SAVE) Program	8/8/2012
USCIS	DHS/USCIS-006 Fraud Detection and National Security Records	8/8/2012
USCIS	DHS/USCIS-011 E-Verify Program	8/8/2012
USCIS	DHS/USCIS-014 Electronic Immigration System-1 Temporary Accounts and Draft Benefit Requests	4/5/2013
USCIS	DHS/USCIS-015 Electronic Immigration System-2 Account and Case Management System of Records	4/5/2013
CBP	DHS/CBP-009 Electronic System for Travel Authorization	7/30/2012
CBP	DHS/CBP-004 Intellectual Property Rights e-Recordation	1/15/2013
CBP	DHS/CBP -002 Global Enrollment System	1/16/2013
CBP	DHS/CBP-018 Customs Trade Partnership Against Terrorism (C-TPAT)	3/13/2013
CBP	DHS/CBP-007 Border Crossing Information (BCI)	5/28/2013
ICE	DHS/ICE-005 Trade Transparency Analysis and Research (TTAR)	9/4/2012
ICE	DHS/ICE-010 Confidential and Other Sources of Information	2/4/2013
ICE	DHS/ICE-007 Alien Criminal Response Information Management System	2/14/2013
ICE	DHS/ICE-014 Homeland Security Investigations Forensic Laboratory System of Records	5/16/2013

Appendix E – Public Speaking Engagements

During this reporting period, the Chief Privacy Officer, the Acting Chief Privacy Officer, and Privacy Office staff spoke on privacy-related issues at the following events:

July 2012

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

October 2012

- American Society of Access Professionals Seminar, Washington, DC

November 2012

- DHS 201 International Attaché Training, Washington, DC
- Electronic Privacy Information Center Privacy Coalition Meeting, Washington, DC

December 2012

- American Society of Access Professionals Symposium, Washington, DC

January 2013

- American University Washington College of Law's Collaboration on Government Secrecy Program, Washington, DC
- Federal Aviation Administration Privacy Week Symposium, Washington, DC
- DHS 201 International Attaché Training, Washington, DC

February 2013

- Privacy and Civil Liberties Oversight Board Meeting, Washington, DC

April 2013

- Public Presentations led by the Executive Order 13636 Integrated Task Force Working Group, Washington, DC
- International Visitor Leadership Program Meeting, Washington, DC

May 2013

- Beyond the Border Executive Steering Committee Meeting, Washington, DC
- Public Presentations led by the Executive Order 13636 Integrated Task Force Working Group, Washington, DC
- American Society of Access Professionals National Training Conference, Washington, DC

June 2013

- Public meetings hosted by the Executive Order 13636 Integrated Task Force Working Group, Washington, DC
- Privacy Office's Annual Privacy Compliance Workshop, Washington, DC
- Government Technology Research Alliance Council Meeting, Cambridge, Maryland
- 2013 Federal CIO Council Boot Camp, Washington, DC
- Georgetown University Law Center Federal Government Practitioners Conference, Washington, DC

Appendix F – Congressional Testimony and Staff Briefings

Congressional Testimony

The Chief Privacy Officer and the Acting Chief Privacy Officer testified at two hearings during the reporting period:

- "State of Federal Privacy and Data Security Law: Lagging Behind the Times?" July 31, 2012, Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Oversight of Government Management.
- "Transportation Security Administration (TSA) Recent Scanner Shuffle: Real Strategy or Wasteful Smokescreen?" November 15, 2012, House Committee on Homeland Security, Subcommittee on Transportation Security.

Congressional Staff Briefings

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

July 2012

- Senate Select Committee on Intelligence: Federated Searches

February 2013

- House Committee on Oversight and Government Reform: Information Sharing
- Senate Committee on the Judiciary: Unmanned Aircraft Systems
- Senate Committee on Homeland Security and Governmental Affairs: Privacy Office Overview

March 2013

- Senate Committee on the Judiciary: Unmanned Aircraft Systems

April 2013

- House Committee on Homeland Security and Governmental Affairs: Fiscal Year 2014 Budget
- House Permanent Select Committee on Intelligence: Arrival and Departure System

May 2013

- Congressional Research Service: Unmanned Aircraft Systems

Appendix G – International Outreach

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

- Australian Department of Immigration and Citizenship
- Citizenship and Immigration Canada
- European Commission
- Finnish Members of Parliament
- French Ministry of Interior
- German Federal Commissioner for Data Protection and Freedom of Information
- German Member of Parliament
- German Members of State Parliaments
- Japanese Cabinet Secretariat
- Japanese Members of Parliament
- Japanese Ministry of Internal Affairs and Communications
- Japanese Ministry of Foreign Affairs
- Justice and Home Affairs Senior Officials Meeting
- New Zealand Ministry of Business, Innovation and Employment
- Norwegian Data Protection Authority
- Office of the European Data Protection Supervisor
- Polish Justice and Home Affairs Counselor
- Public Safety Canada
- United Kingdom Home Office