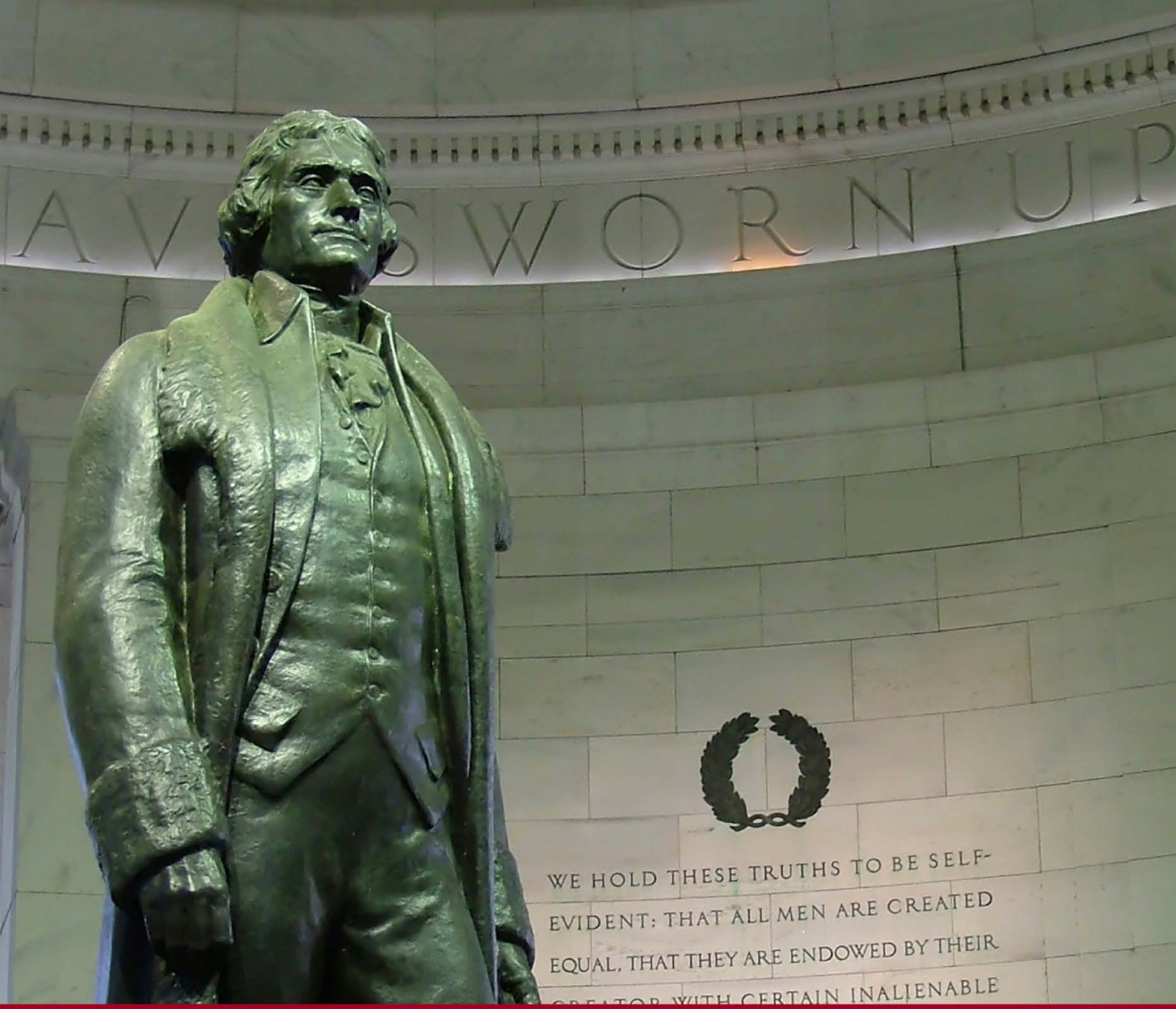


DHS Privacy Office

Annual Report to Congress

July 2010 – June 2011

September 2011

Homeland Security

Message from the Chief Privacy Officer

The Department of Homeland Security Privacy Office (DHS Privacy Office or Office) is proud to present its seventh Annual Report covering the period from July 2010 through June 2011. This report, as well as previous reports, can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

I am moving into my third year as the DHS Chief Privacy Officer, and am pleased with the improvements the DHS Privacy Office has made in strengthening privacy protections in Department operations while concurrently fulfilling the Administration's goals of transparency, public participation, and collaboration. In short, the DHS Privacy Office has made a difference in how the Department carries out its mission of protecting the American people. For example, we have developed core teams in the DHS Privacy Office to address privacy at each stage of a program's life cycle—creation, development, implementation, Department-wide application and policy consideration, and termination. We also work closely with our colleagues who have primary responsibility for handling Personally Identifiable Information (PII). Furthermore, as of the close of this reporting period there are full-time, senior privacy officers in all of the operational components. Developing a cadre of component privacy officers who are steeped in both the operations of their individual components and in privacy expertise multiplies the DHS Privacy Office's ability to implement consistent privacy practices across the Department's vast and varied operations. In sum, the Department now has over 100 dedicated privacy professionals working in privacy offices in the Department, in addition to the strong support we receive from program managers and executives throughout the Department. Having such an amazing depth of privacy expertise allows us to be involved throughout the entire lifecycle of the Department's programs.

In addition, we continue to support the Administration's efforts to promote openness, transparency, and public participation. The institution of our Proactive Disclosure Policy means that certain categories of documents are now published on the headquarters and component websites, eliminating the need for the public to file Freedom of Information Act requests for those documents. Making documents readily available increases the ability of the public to be informed about Department operations. At the same time, we remain stewards of the individuals we serve. We strive diligently to create an environment where privacy and security are not traded or balanced, but integrated in a manner that keeps this country safe and honors the principles on which the country was founded.

In that spirit, we actively lead privacy policy development across the federal government through leadership positions in all of the federal privacy organizations. When issues arise that affect the federal government as an enterprise, the DHS Privacy Office staff utilizes those opportunities by serving as a voice for privacy protections. This year, we have done so with regard to the use of cloud computing technology, social media, identity management, and other developing areas with privacy implications.

The scope of DHS's mission also demands that the DHS Privacy Office take a leading role in the international privacy dialogue. In the past year, we conducted significant outreach efforts with our international partners to enhance their understanding of the U.S. privacy framework and DHS privacy policy and procedures. We also continue to provide vital guidance to the Department and interagency partners on privacy implications of international agreements as well as guidance on international privacy policy.

I look forward to continuing to lead the charge to enhance privacy protections and promote government transparency and accountability not only in the Department but also in the federal government and international community, and foresee an even more productive future.

Mary Ellen Callahan
Chief Privacy and Freedom of Information Act Officer
United States Department of Homeland Security

Executive Summary

The DHS Privacy Office is the first statutorily created privacy office in any federal agency, as set forth in Section 222 of the Homeland Security Act, as amended.[1] The mission of the DHS Privacy Office is to preserve and enhance privacy protections for all individuals, to promote transparency of DHS operations, and to serve as a leader in the federal and international privacy communities. The Office accomplishes its mission by focusing on several core activities:

- Requiring compliance with the letter and spirit of 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.
- Ensuring transparency to the public through published materials, reports, formal notices, public workshops, and meetings.

During the course of the reporting year, the DHS Privacy Office has built upon the initiatives addressed in last year's report and has played an important role in an expansive breadth of privacy and FOIA-related issues throughout the Department, the federal community, and with international partners. The continued leadership of the DHS Privacy Office is exemplified in many areas.

Accomplishments within DHS:

- Approved and published 68 Privacy Impact Assessments (PIAs) and 20 System of Records Notices (SORNs), on Department programs, systems, and initiatives.
- Developed a DHS "Privacy Policy and Compliance" Management Directive reinforcing Department privacy policy based on the FIPPs and detailing privacy-related responsibilities of all DHS employees.
- Enhanced privacy training and awareness by launching a new intranet site featuring the Office's privacy and FOIA training resources, distributing a two-page factsheet detailing best practices for safeguarding Sensitive PII, developing a new online *A Culture of Privacy Awareness* annual mandatory training course, and providing guidance to components developing component-specific privacy training.
- Investigated, mitigated, and closed 88% of reported privacy incidents.

[1] 6 U.S.C. § 142.

- Used the Chief Privacy Officer's statutory investigative authority under Section 802 of the 9/11 Commission Act for the first time, to investigate and then publish a report and recommendations on a privacy incident involving the DHS Office of Inspector General (OIG) and KPMG, a DHS contractor.
- Reviewed all new DHS information sharing agreements involving PII being shared outside of DHS, and ensured application of the FIPPs to protect PII and comply with DHS policy.
- Issued a new Privacy Policy Guidance Memorandum entitled *Roles & Responsibilities for Shared IT Services*, signed by the Chief Privacy Officer, the Chief Information Officer, the Assistant Secretary for Policy, and the Director of Records.
- Participated on the newly formed DHS Identity, Credential, and Access Management Executive Steering Committee, which is the Department's core oversight and advisory body for ensuring implementation of the Department's Identity, Credential, and Access Management program.
- Continued its review of privacy policies at fusion centers to ensure that they are "at least as comprehensive" as the Information Sharing Environment Guidelines. As of March 2011, all 71 officially designated fusion centers have policies satisfying these requirements.
- Collaborated with the Department's Office for Civil Rights and Civil Liberties to train fusion center staff nationwide on privacy law, privacy requirements, and Department privacy policy.
- Initiated an annual review of the Department's FOIA operations, and coordinated the first Department-wide FOIA workshop for DHS personnel.
- Initiated an assessment of the Department's National Cybersecurity Protection System and collaborated with the DHS National Protection and Programs Directorate's (NPPD's) Office of Privacy to develop a strategy for assessing the privacy impacts of the Department's overall cybersecurity program.
- Provided transparency to the public through meetings with the privacy advocacy community, 33 public speaking engagements, and the DHS Blog.

Accomplishments in the Federal Community:

- Supported efforts by the National Security Staff and NIST to develop the National Strategy for Trusted Identities in Cyberspace (NSTIC) by participating in the drafting and launch of the NSTIC and successfully advocating for NSTIC's adoption of the FIPPs as the benchmark for evaluating privacy impacts in online identity management applications.
- Participated directly in negotiations of several major information sharing agreements, including evaluation of information sharing requests, with various information sharing partners, including the National Counterterrorism Center (NCTC), and the Departments of State, Justice, and Defense.

- Conducted a two-day Privacy Compliance Workshop that addressed both compliance basics for federal personnel new to privacy issues and advanced content for seasoned federal privacy professionals.
- Played a lead role in ensuring that privacy requirements received prominent coverage in the foundational documents for the Administration's Open Government Initiative, and led the development of privacy criteria for the use of those credentials by federal agencies;
- Provided guidance to the Departments of State and Agriculture, the Federal Aviation Administration, and the U.S. Government Printing Office on their respective privacy incident response programs.
- Collaborated with the Department of Justice's Office of Information Policy to offer in-depth training on the proper application of FOIA Exemption (b)(2) following the United States Supreme Court's narrowing of the exemption in *Milner v. Department of the Navy*.

Accomplishments in the International Community:

- Provided considerable privacy expertise during ongoing negotiations of significant international agreements as part of DHS and United States Government negotiating teams to ensure consistency with U.S. privacy law and policy. Examples include negotiations of the U.S. – EU Passenger Name Record Agreement, the U.S. – EU Data Protection and Privacy Agreement, and the Five Country Conference.
- Encouraged international partners to adopt privacy best practices, such as implementation of internationally recognized FIPPs, and to use model compliance documents, such as the DHS PIA, to implement bilateral and multilateral information sharing arrangements.
- Contributed to a major review of the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines by sponsoring a study on how the Guidelines influenced the development of laws, regulations, and public policy in select OECD member states.
- Participated in programs for international visitors learning about the U.S. privacy framework and created privacy training modules for internationally deploying U.S. Government Foreign Service officials to enhance their understanding of international privacy policy issues.

Figure 1 depicts the implementation elements that comprise the culture of privacy at DHS. Each of the eleven elements makes an important contribution to the development of a privacy culture; and the privacy activities described in this annual report often touch on more than one of these elements. The Culture of Privacy graphic appears at the beginning of each section of the report to indicate which element(s) the section addresses.

Figure 1: Culture of Privacy Implementation Elements

Table of Contents

List of Figures

List of Tables

Legislative Language

This Report has been prepared in accordance with the Homeland Security Act of 2002, 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

A. About the Office

The DHS Privacy Office's mission is to preserve and enhance privacy protections for all individuals, to promote transparency of DHS operations, and to serve as a leader in the privacy community. As described in this July 1, 2010 - June 30, 2011 Annual Report (Report), the Office has made a difference —– both domestically and internationally —– by enhancing a culture of privacy at DHS while also supporting the Department's complex mission.

All of the Office's efforts have built, and continue to sustain, a culture of privacy at the Department. One of the cornerstones of that culture is the Office's translation of the Fair Information Practice Principles (FIPPs) into concrete and proactive policies and procedures as presented in Figure 2.[2]

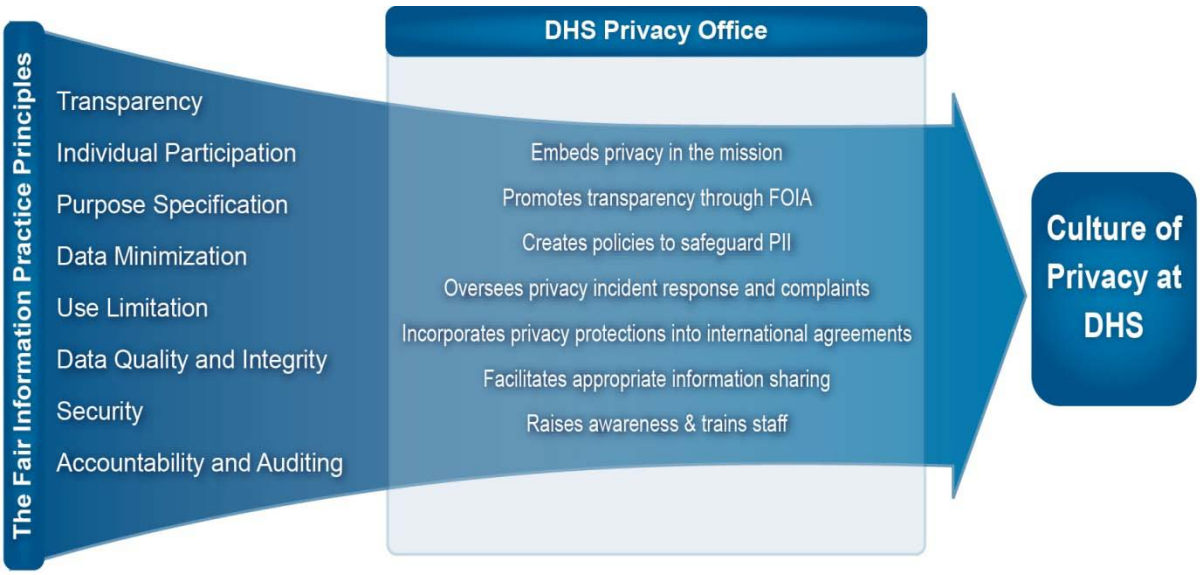


Figure 2: DHS Privacy Office Overview

FOIA embodies the principle that individuals have a fundamental right to know what their government is doing and what information it holds about them. Due to the symbiotic

[2] The FIPPs are rooted in the Privacy Act of 1974, 5 U.S.C. 552a (Privacy Act) 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 FIPPS are set out in Appendix I.

relationship between privacy and FOIA, the Chief Privacy Officer is also the Chief FOIA Officer for the Department.

The DHS Privacy Office undertakes its statutory and policy-based responsibilities in a collaborative environment with DHS component privacy officers, privacy points of contact (PPOCs),[3] and program offices to ensure that all privacy and disclosure issues receive the appropriate level of review and expertise.

The Office accomplishes its mission by:

- requiring compliance with the letter and spirit of federal privacy and disclosure laws and policies in all DHS programs, systems, and operations;
- centralizing FOIA and Privacy Act operations to provide policy and programmatic oversight, to support DHS component FOIA operations, and to ensure the consistent handling of disclosure requests;
- providing leadership and guidance to promote the culture of privacy and adherence to the FIPPs across the Department;
- conducting investigations of privacy incidents in the Department and determining required steps to mitigate them and prevent their recurrence;
- advancing privacy protections, transparency and accountability 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.

B. Growth this Year

The DHS Privacy Office continues to fulfill its mission and contribute to the Department's mission by ensuring that it is appropriately staffed to support the increasing responsibilities and coordination required. In Fiscal Year (FY) 2011, the Office received an appropriation of $8.103 million.[4] As of June 2011, the Office staff includes 45 full-time equivalents and a part-time intern. One full-time contractor and three part-time contractors also support the Office.

During FY 2011, the Office added three new senior-level positions in order to help support the Office's increased responsibilities. The new positions are:

- Deputy Chief FOIA Officer serves as the key adviser to the Chief Privacy Officer and other senior DHS leadership on compliance with FOIA, the Privacy Act, and other DHS

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

[4] FY 2011 funding excludes a one-time increase in the amount of $303,074 to cover GSA rent adjustments. The reporting period for this report runs from July through June, while the Department's fiscal year runs from October through September.

authorities, policies, programs, and agreements that promote government transparency and accountability;

- Chief of Staff is responsible for managing the Office's budget, administrative functions, personnel, and continuity of operations; and
- Associate Director for Incidents and Inquiries works closely with the Director, Privacy Incidents and Inquiries to manage the DHS-wide privacy incidents and inquiries program and conduct investigations into breaches and misuse of PII.

Also during this reporting period, the DHS Privacy Office converted contractor resources to hire a FOIA Program Specialist, a Senior Privacy Analyst, two Program Analysts, and an Administrative Specialist to augment the current federal staff. As noted later in this Report, DHS receives the largest number of FOIA requests of any department in the federal government. The additional FOIA staff, to include the Administrative Specialist, will enable the Office to handle the high volume of FOIA and Privacy Act requests and to provide support to DHS components as needed. The Senior Privacy Analyst and the Program Analysts will enhance the Office's ability to provide privacy subject matter expertise on Department information sharing and access agreements, homeland intelligence reports, intelligence products, and policy development.

C. About this Report

This is the DHS Privacy Office's seventh Annual Report to Congress. It covers the period July 1, 2010 through June 30, 2011.

During the reporting period, two overarching objectives have guided the work of the DHS Privacy Office. First, consistent with its legal authorities and the FIPPs, the Office has continued to focus on implementing effective privacy and disclosure protections throughout DHS and in the Department's agreements with other federal agencies and with international partners. Second, the Office has led concerted DHS efforts to enhance accountability and implement effective transparency into the Department's operations, as required by President Obama's Open Government Initiative and the FIPPs' transparency principle.

Part One of this Report discusses the DHS Privacy Office's and DHS components' ongoing leadership in operationalizing privacy throughout the Department and across the federal government. It describes the DHS Privacy Office's work in privacy compliance, privacy policy, privacy incident response, oversight of DHS' information sharing practices and intelligence practices, and the Department's use of technology. It also describes the Office's central role in privacy policy development across other federal departments and agencies, and highlights the privacy education and training the DHS Privacy Office provides for Department employees. Part One concludes with a description of privacy initiatives undertaken by the components to promote a culture of privacy at DHS.

Part Two of this Report describes the DHS Privacy Office's achievements in enhancing accountability and transparency across Department operations. It details the Office's FOIA-related activities and other work in furtherance of the Open Government Initiative. It then provides updates on the DHS Privacy Office's work on privacy issues associated with DHS redress programs, and on the Office's and the components' management of privacy complaints during the reporting period. Part Two concludes by summarizing the DHS Privacy Office's

public reporting on DHS activities and the work of the DHS Data Privacy and Integrity Advisory Committee (DPIAC).

Part Three of this Report provides an overview of the extensive efforts of the DHS Privacy Office in international matters over the past year. It describes the Office's multi-faceted outreach to enhance the Department's international partners' understanding of the U.S. privacy framework and implementation of DHS privacy policy, the Office's leadership in addressing the privacy implications of international agreements, and its advice on interpreting international privacy frameworks.

The Report concludes with a brief look into the future of privacy at DHS and the role of the DHS Privacy Office going forward.

Part One – Making a Difference: Operationalizing Privacy Protections

During this reporting period, the DHS Privacy Office made a difference and contributed to the Department's mission by actively promoting DHS privacy policy and compliance through internal collaboration, oversight, and outreach. The Office also led federal inter-agency privacy policy development through numerous engagements, thus also helping to make a difference within the federal privacy community. Part One of this Report discusses the myriad ways in which the Office achieved these accomplishments.

I. Compliance Activities

The DHS Privacy Office Compliance Group (led by the Director of Compliance and two Associate Directors) (Compliance Group) ensures privacy protections are built into Department systems, initiatives, and programs as they are developed and modified. The Compliance Group provides public transparency into Department operations by supervising and approving all DHS privacy threshold analyses (PTAs), privacy impact assessments (PIAs), and system of records notices (SORNs) and following up on implementation and compliance with those privacy compliance documents. The Compliance Group's activities demonstrate that privacy protections are maturing throughout the Department.

The following are highlights of three key PIAs approved during this reporting period.

- DHS Information Sharing Environment (ISE) Suspicious Activity Report (SAR) Initiative - The DHS Information Sharing Environment SAR Initiative PIA incorporates baseline privacy protections into this DHS-wide initiative, such as specific privacy training, elimination of unnecessary PII, and reviews to ensure reporting adheres to legal authority and the Initiative's mission.

- E-Verify Self Check PIA - The E-Verify Self Check PIA ensures privacy protections are integral to the Self Check system, which provides individuals direct access to proactively review and, if necessary, correct work authorization status to ensure information is accurate before a potential employer conducts a status check. The PIA is the result of significant collaboration between the DHS Privacy Office and the E-Verify program office since the inception of the program. The Self Check service uses a third party Identity Proofing (IdP) Service to authenticate the individual user's identity prior to accessing the individual's work authorization status. The Privacy Office worked closely with the E-Verify program office to ensure the use of the IdP was consistent with privacy principles and policies, including standards that allow IdP to authenticate individuals without conveying any additional PII to the E-Verify program office.

- U.S. Customs and Border Protection (CBP) TECS[5] PIA - The CBP TECS PIA addresses privacy issues in CBP's main IT system containing PII about individuals crossing the U.S. borders. The PIA is the result of extensive collaboration between CBP and the Compliance Group.

The Compliance Group uses PIAs to establish rules based on the FIPPs for Department programs, systems, and initiatives. The Compliance Group is also responsible for seeing that the Department meets statutory requirements such as the Federal Information Security Management Act of 2002 (FISMA)[6] privacy reporting, Section 803 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) reporting, OMB 300 reviews, Enterprise Architecture Board (EAB) reviews, other compliance reviews, and for conducting outreach to the component privacy officers and PPOCs to ensure that privacy compliance requirements are met.

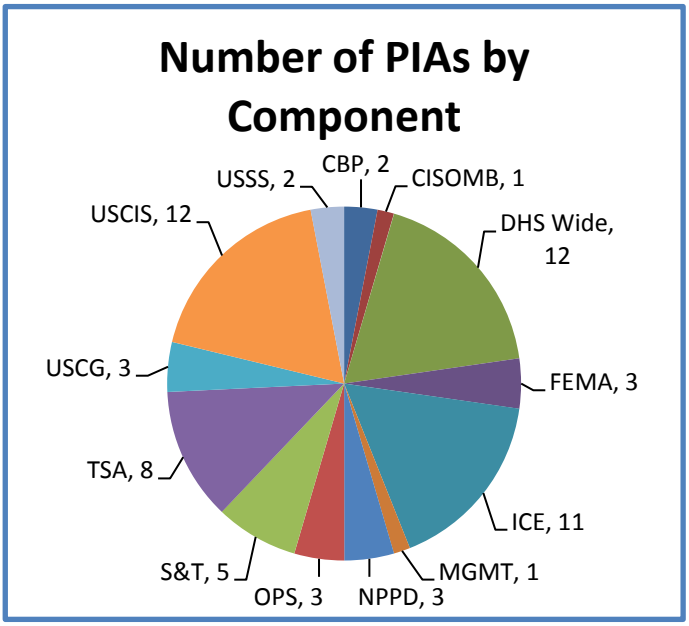


Figure 3: Number of PIAs Completed by Component during the Reporting Year

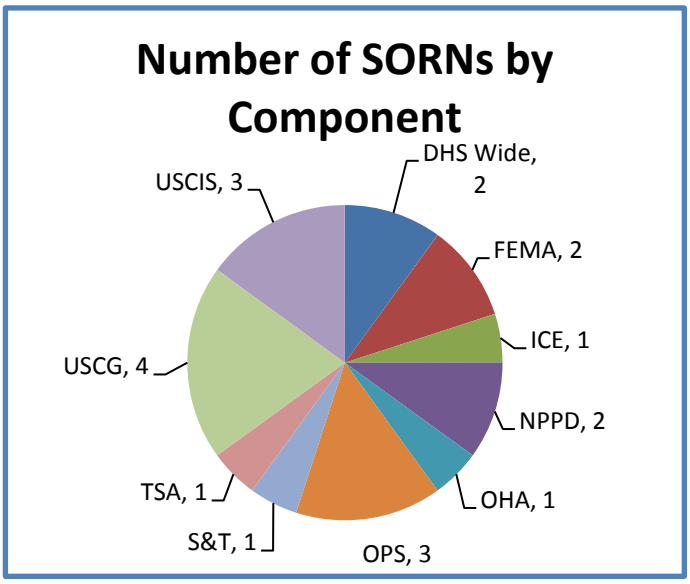


Figure 4: Number of SORNs Completed by Component during the Reporting Year

A compendium of PIA abstracts is published in the Federal Register on a periodic basis.[7] Between July 1, 2010 and June 30, 2011, the Chief Privacy Officer approved and published 66 PIAs. Figure 3 illustrates the number of PIAs completed by each component during this reporting year.

Figure 4 depicts the number of SORNs published during the reporting year, by component. During the reporting period, the Chief Privacy Officer approved and published 20 SORNS. Lists of PIAs and SORNs

[5] When the SORN for the former Treasury Enforcement Communication System was published under DHS on December 19, 2008, the system was renamed TECS.
[6] 44 U.S.C. § 3544.
[7] PIAs are posted on the DHS Privacy Office website: www.dhs.gov/privacy, under the link to Privacy Impact Assessments.

approved during this reporting period are included in Appendix I.C and D. PIAs approved during this reporting period that were either redacted in part or withheld from publication due to Law Enforcement Sensitive information are listed in an Annex to this Report that is being provided separately to the Congress.

The Compliance Group demonstrates its leadership in federal privacy compliance by setting best practices through DHS PTA, PIA, and SORN templates and guidance that are then leveraged by other government agencies. The Compliance Group conducts an annual Compliance Workshop that is open to the public. Attendees include DHS, other federal government privacy professionals, and private sector professionals. In this reporting year, the Compliance Group extended the workshop to two days. The first day covered privacy compliance basics, and the second day addressed advanced content for seasoned privacy professionals. This free, high-value forum is an opportunity for all privacy practitioners to share lessons learned and best practices, and to advance privacy throughout the government.

Social Media Policy and Compliance

As part of the Administration's Open Government Initiative, the Department actively adopted the use of social media. In support of that effort, the Compliance Group issued a Department-wide policy to ensure the protection of PII while using social media. During this reporting period, the Government Accountability Office (GAO),[8] media, and citizens recognized DHS for its Department-wide PIAs on the use of social media and the privacy policies posted on the Department's public-facing website. Systems, initiatives, or programs that want to use social media must now submit a specialized social media PTA indicating their intent to comply with a DHS-wide social media PIA as well as a draft of the privacy policy to be made available to public users before launch. The Department's use of social media requires that legal, accessibility, privacy, communications, information security, and records management considerations be addressed before launching social media tools and initiatives. The required protections help program managers design social media initiatives to minimize PII collection and allow the public to interact with the Department online without compromising privacy.

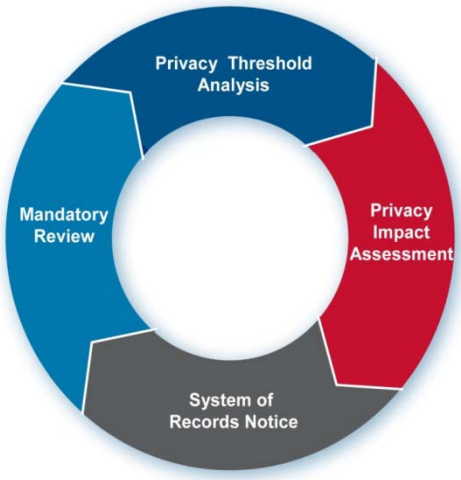


Figure 5: DHS Privacy Office Compliance Process

The Compliance Group continues to work proactively with the DHS Office of the General Counsel (OGC), Office for Civil Rights and Civil Liberties (CRCL), Office of Public Affairs, Chief Information Security Office (CISO), and Records Management Office to comprehensively review policies, plans, and supporting documentation that govern the use of social media at DHS.

[8] The GAO report, GAO-11-605, entitled *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, is available at http://www.gao.gov/new.items/d11605.pdf.

Privacy Compliance Reviews

During this reporting period, the Compliance Group extended its use of Privacy Compliance Reviews (PCRs) to Departmental initiatives with potentially high privacy impacts. Consistent with the Privacy Office's unique position as both an advisor and oversight body for the Department's privacy-sensitive programs and systems, the PCR is a constructive mechanism that improves a program's ability to comply with assurances made in existing PIAs, SORNs, and other formal agreements.

The Compliance Group conducted two public PCRs for the Department's Media Monitoring Initiative. The DHS Office of Operations Coordination and Planning (OPS), including the National Operations Center, launched the Social Networking/Media Capability to assist DHS and its components involved in security, safety, and border control associated with the 2010 Winter Olympics. The Initiative also monitored the response, recovery, and rebuilding effort resulting from the earthquake and after-effects in Haiti. The two PCRs for this Initiative, conducted at major development points, confirmed all parties were generally in compliance, and recommended improvement for accountability.[9] The Privacy Office's continued coordination with OPS and review of Media Monitoring Initiative demonstrates the Department's ongoing compliance.

Appendix II.A contains further information on the Compliance Group's work, including a description of the DHS Privacy Office's process for reviewing PTAs, PIAs, and SORNs.

[9] The two PCRs are available through www.dhs.gov/privacy. Media Monitoring Initiative is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_ops_monitoring_initiative.pdf; Haiti Social Media Disaster Monitoring Initiative and 2010 Winter Olympics Social Media Event Monitoring Initiative is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy-privcomrev-ops-olympicsandhaiti.pdf.

II. Privacy Policy

During this reporting year, the DHS Privacy Office's Policy Group (Policy Group) (led by the Director of Privacy Policy, the Associate Director of Privacy Policy and the Associate Director of Communications and Training) has been actively engaged in an array of policy, training and communications initiatives both inside and outside the Department. The Policy Group has been a leader on the Office's behalf in several high-profile cross-governmental efforts. The Policy Group collaborated with colleagues in the Office and with component privacy officers and PPOCs on diverse policy, training, and communications issues. These efforts strengthened privacy protections and the culture of privacy within DHS, and ensured that privacy was effectively addressed in several federal government-wide initiatives.

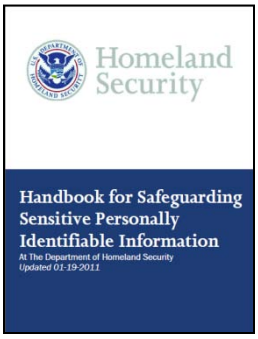
During the reporting period, the Policy Group:

- developed a DHS "Privacy Policy and Compliance" Management Directive reinforcing Department privacy policy based on the FIPPs and detailing privacy-related responsibilities of all DHS employees, led by the Chief Privacy Officer;
- played a lead role in ensuring that privacy requirements received prominent coverage in the foundational documents for the Administration's Open Government Initiative. A key goal of this initiative is leveraging private sector identity credentials for accessing federal government websites and information. The Policy Group led the development of privacy criteria for the use of those credentials by federal agencies, thus advancing the Administration's goals while ensuring that PII is protected;
- collaborated with inter-agency colleagues to prepare a draft appendix of privacy controls for the National Institute of Standards and Technology's (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, which will be finalized later this year.[10] Taken together, the security and privacy controls will provide comprehensive guidance to federal IT professionals, and to their colleagues with privacy policy responsibilities, on implementing the full range of privacy protections for PII held by federal agencies;
- collaborated with the Federal Emergency Management Agency (FEMA) staff to extend the reach of DHS privacy policy by recommending in official guidance that all recipients of FEMA Preparedness Grants who collect PII have a publicly-available privacy policy;[11]

[10] The draft Appendix is available at http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf.

[11] FEMA *Grant Program Directorate (GPD) Preparedness Grant Programs Guidance and Application Kit Section II (Award Administration Information)* (May 2011) at p. 6, available at http://www.fema.gov/pdf/government/grant/2011/fy11_nsgp_award.pdf.

- enhanced privacy training for DHS staff and contractors through ongoing redevelopment of the mandatory *A Culture of Privacy Awareness* online course. The new course, to be available in FY 2012, will use "real world" scenarios to convey the importance of protecting Sensitive PII and guidance on how to do so. Part One, Section VII and Appendix II.D include more information on the *A Culture of Privacy Awareness* training;
- revised and reissued the DHS *Handbook for Safeguarding Sensitive Personally Identifiable Information* (*SPII Handbook*). The revisions clarify and strengthen procedural safeguards for protecting Sensitive PII when it is not in use. The revised *SPII Handbook* is posted on the DHS Privacy Office's public-facing website and distributed to all DHS employees through the Office's intranet site. In addition, a two-page summary of the *SPII Handbook* was created as a training tool that will be conveyed to all DHS staff via the new *A Culture of Privacy Awareness* course; and



- provided cogent and timely guidance on an array of privacy and privacy-related matters to officials throughout the Department upon request.

The Policy Group will continue to build on this year's efforts and accomplishments in the next reporting year, to help further embed privacy throughout the Department, and to support government-wide efforts.

III. Privacy Incidents and Inquiries

Managing privacy incident and complaint response is a cornerstone of the DHS Privacy Office's commitment to enhancing the culture of privacy at DHS. Led by the Director and Associate Director of Privacy Incidents and Inquiries, the Privacy Incidents and Inquiries Group directs the Privacy Incident Management program in collaboration with the DHS Enterprise Operations Center (EOC), component privacy officers and PPOCs, and DHS management.[12] The Privacy Incidents and Inquiries Group works to ensure all incidents are properly reported, and mitigation and remediation efforts are appropriate for each incident. The Privacy Incidents and Inquiries Group also leads the DHS Privacy Office's efforts relating to investigations of privacy incidents and privacy policy violations throughout the Department. The Chief Privacy Officer released her first public investigative report during this reporting period following the loss of Sensitive PII by a DHS contractor. The Privacy Incidents and Inquiries Group also engaged in extensive intra- and inter-agency collaboration.

A. Incident Response

During this reporting period, the majority of incidents affected a small number of individuals and data, while a select few incidents involved larger number of individuals and data. The DHS Privacy Office believes that the reduction in large-scale breaches is due, in part, to enhanced privacy awareness training throughout the Department that focuses on preventing privacy incidents. Incident mitigation and remediation is coordinated among the DHS Privacy Office, DHS EOC, component privacy officers and PPOCs, and Information Systems Security Managers. During the reporting period:

- 449 privacy incidents were reported to the DHS EOC during the reporting period; and
- DHS investigated, mitigated, and closed 396 or 88% of the reported privacy incidents.

Table 1 depicts the number and type of incidents reported during the past two years.

[12] The Privacy Incidents and Inquiries Group also oversees the Department's review of privacy complaints, as discussed in Part Two, Section II.A of this Report.

Type of Incident[13]	Number of Incidents: July 1, 2010 to June 30, 2011	Number of Incidents: July 1, 2009 to June 30, 2010
Alteration/Compromise of Information	369	239
Classified Computer Security Incident	3	2
Investigation Unconfirmed/Non-Incident	49	19
Malicious Logic	2	0
Misuse	20	10
Unauthorized Access (Intrusion)	6	8
Probes and Reconnaissance Scans	0	1
Total[14]	***449***	***279***

Table 1: DHS Privacy Incidents Reported

DHS has established a standing Core Management Group (CMG) that meets annually to evaluate and discuss privacy incidents and incident handling procedures. The DHS CMG includes the Chief Privacy Officer, representatives of 13 DHS headquarters offices, and lead offices for affected components.

In September 2010, the Chief Privacy Officer hosted the second annual CMG Meeting. The Privacy Incidents and Inquiries Group presented the Department-wide privacy incident handling program metrics, accomplishments, and ongoing efforts. The meeting provided an overview of the privacy incident handling program and detailed overall DHS and component successes in identifying, reporting, and mitigating privacy incidents from January 2007 through August 2010.

B. Investigative Activity

Congress expanded the authorities and responsibilities of the Chief Privacy Officer in 2007 in Section 802 of the 9/11 Commission Act, which added investigatory 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.

During the reporting period, the DHS Privacy Office completed its first investigation using its statutory investigative authority. The investigation concerned a privacy incident involving the DHS Office of Inspector General (OIG), several DHS components, and KPMG, a DHS contractor. The incident involved the loss of an unencrypted flash drive containing DHS financial records audit data, including Sensitive PII, from several DHS offices and components. KPMG had compiled the data during the FY 2009 audit it conducted for the OIG.

In February 2011, the Chief Privacy Officer published a report on the investigation entitled *DHS Privacy Office OIG Privacy Incident Report and Assessment.*[15] The Report includes findings and recommendations addressing compliance with privacy policies and recommends steps for prevention and mitigation of similar privacy incidents. The recommendations encompassed

[13] The types of incidents are detailed in NIST Special Publication 800-61 (Rev.1), *Computer Security Incident Handling Guide*, available at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf. Definitions of each type of incident are located in Appendix II.B.

[14] The increase in the number of incidents is partly attributable to changes in reporting the loss of Blackberrys and laptops. The policy change evolved over the first four months of 2011.

[15] The Report, *DHS Privacy Office OIG Privacy Incident Report and Assessment* is available at http://www.dhs.gov/xlibrary/assets/privacy/priv-oig-privacy-incident-report-assessment-022011.pdf.

contracting practices for handling Sensitive PII, data minimization, data security, and privacy training. The report recommended that:

- DHS contracts contain clauses or provisions to safeguard against disclosure and inappropriate use of all potential types of sensitive information to include Sensitive PII that contractors might access, create, or maintain during contract performance. This includes the responsibility for prompt notification to the agency if unauthorized disclosure or misuse of Sensitive PII occurs;
- [a]ll [contracting officers] improve monitoring of contractor compliance with contract provisions to ensure roles and responsibilities regarding data protection and privacy compliance are executed properly;
- [c]omponents participating in the audit reviews revise their Financial Management Directives, Financial Audit Responses to Document Requests to ensure the responsibilities and procedures regarding the proper review, collection and transmission of PII are addressed;
- [c]omponents that experience a Privacy Incident involving another component's PII should immediately notify the affected component privacy officer and continually coordinate the incident response strategy; and
- DHS enforce the existing policy as stated in DHS Policy Directive 4300A Policy I.D. 4.3.1 [*DHS Sensitive Systems Policy Directive 4300A*[16]]. DHS should continue to require DHS flash drives be encrypted whenever used by DHS employees, contractors, or other persons with access to Sensitive PII. Whenever flash drives are utilized, components should implement chain of custody procedures to ensure accountability for flash drives that contain Sensitive PII.[17]

C. Collaboration

During this reporting period, the Privacy Incidents and Inquiries Group engaged in extensive collaboration both within and outside the Department. The Group:

- met with three DHS components to discuss best practices and determine the most efficient and effective processes for managing privacy incidents, safeguarding PII, and addressing other privacy issues;
- met with EOC personnel twice to refine the privacy incident management online tracking system. The visits yielded immediate improvements by creating a more efficient tracking system;
- met with privacy officials from the Office of the Public Printer, U.S. Government Printing Office (GPO) in October 2010, to provide assistance and guidance regarding GPO's development and implementation of a privacy incident response plan;

[16] DHS 4300A *Sensitive Systems Handbook* outlines procedures to assist components as they implement the DHS Information Security Program policies for sensitive systems contained in DHS Sensitive Systems Policy Directive 4300A.
[17] *Id.* at 25-26.

- collaborated in April 2011, with the Department of State to address an interagency privacy incident that affected DHS and other federal agencies. This collaboration allowed the DHS Privacy Office to recommend mitigation efforts to ensure timely notification of affected individuals, and to address Frequently Asked Questions;
- provided assistance to officials from the Federal Aviation Administration (FAA) and the Department of Agriculture on their privacy incident response programs; and
- continued to monitor the reporting system and request modifications to the online reporting process as needed.

IV. Privacy Information Sharing and Intelligence

The DHS Privacy Office's oversight and support responsibilities are perhaps nowhere more critical than in the area of DHS information sharing and intelligence activities. During the reporting year, the newly-formalized Privacy Information Sharing and Intelligence (PISI) Group provided essential privacy guidance in reviews of information sharing agreements, DHS intelligence products, and state and major urban area fusion center privacy policies. Together with CRCL, the Office continued to provide comprehensive training to fusion center staff and DHS intelligence professionals assigned to the fusion centers. The PISI Group's collaboration with component privacy offices, the DHS Office of Intelligence and Analysis (I&A) staff, and external sharing partners integrated privacy protections into information sharing and intelligence processes and ensured that the Department executes its information sharing and intelligence functions in a privacy-protective manner. Highlights of each area are detailed below.

A. Information Sharing and Access Agreements

The PISI Group continued to provide timely and results-oriented privacy analysis to embed privacy protections into information sharing arrangements within the Department and with federal, state, local, tribal, and private sector partners. During the reporting period the PISI Group:

- participated directly in negotiations of several major information sharing agreements, including evaluation of information sharing requests, with various information sharing partners, including the National Counterterrorism Center (NCTC), and the Departments of Defense, State, and Justice;
- reviewed all new information sharing agreements involving PII being shared outside of DHS, and ensured application of the FIPPs to protect PII and comply with DHS policy;
- conducted compliance reviews during each information request evaluation, and subsequently updated three PIAs;[18] and
- provided subject-matter expertise in support of international information access sharing agreements to ensure inclusion of privacy protections for personal information.

[18] The three PIAs (Advanced Passenger Information System (APIS), Student and Exchange Visitor Information System (SEVIS), and Refugees, Asylum, and Parole System (RAPS)) are available at www.dhs.gov/privacy, and document number is provided in Appendix I.

B. Information Sharing Policy Leadership

The DHS Privacy Office has maintained its leadership role in advancing privacy protections through the development of sound information sharing policies, both within DHS and across the federal government. During this reporting year the PISI Group:

- supported efforts by the National Security Staff (NSS) and NIST to develop the National Strategy for Trusted Identities in Cyberspace (NSTIC) by participating in the drafting of and launch of the NSTIC, successfully advocating for NSTIC's adoption of the FIPPs as the benchmark for evaluating privacy impacts in online identity management applications. The PISI Group will continue to work with NSS and NIST to implement the NSTIC during the next reporting year;
- participated in the development of several key new DHS information sharing policies, including DHS-wide guidance for response to requests for information from elements of the intelligence community;
- supported the Chief Privacy Officer in her role as an *ex officio* member of the DHS Information Sharing Governance Board; and
- participated in five Information Sharing and Access Interagency Policy Committee (ISA-IPC) subcommittees: Privacy and Civil Liberties Subcommittee, Fusion Center Subcommittee, Suspicious Activity Reporting Subcommittee, Watchlisting and Screening Subcommittee, and Information Integration Subcommittee. More information about each subcommittee, and the Privacy Office's role in each, is included in Appendix II.C.

C. Support for Fusion Centers

In 2007, Congress established the DHS State, Local, and Regional Fusion Center Initiative--codifying an existing relationship between DHS and a national network of fusion centers--in the 9/11 Commission Act. As detailed in last year's Annual Report, the DHS Privacy Office has exercised leadership in establishing and growing a robust privacy protection framework within the fusion center program, both at the national and state levels. During this reporting period the PISI Group:

- continued its review of privacy policies at fusion centers to ensure that they are "at least as comprehensive" as the Information Sharing Environment (ISE) Guidelines.[19] By March 2011, all 71 officially designated fusion centers had policies satisfying these requirements. Secretary Napolitano recognized this important milestone during her keynote speech at the 2011 National Fusion Center Conference;

[19] The Office supported these efforts in several ways, such as having the Chief Privacy Officer co-chair the Privacy and Civil Liberties Subcommittee of the ISA-IPC, the body that issues and manages ISE Privacy Guidelines implementation. The Office led efforts to recommend the standard is communicated to fusion centers through the Global Baseline Capabilities document, and the Chief Privacy Officer was instrumental in getting FEMA's FY 2010 Grant Guidance to address the requirement. Specifically, the grant guidance stated that FY 2010 DHS grant funds cannot be used to support fusion center initiatives unless the center can certify that privacy civil rights and liberties are in place within six months of the award date. Without that certification by March 2011, grant funds could only have been used to develop and complete the privacy protections requirement. For more information see page 35 of the 2010 Annual Report, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf.

- participated in the Department's Senior-level Fusion Center Advisory Group. This group is chaired by the Principal Deputy Under Secretary for I&A and is comprised of high-ranking officials from the Department's operational components and other Departmental stakeholders. Such high-level participation ensures a coordinated Department-wide approach to working with the National network of fusion centers. The Privacy Office's membership on this group helps ensure there is Department-wide support for, and an awareness of, the Office's work to establish a strong privacy protection framework within fusion centers across the nation;
- coordinated training, oversight, and other interactions with fusion centers by working with the DHS State & Local Program Office (SLPO), an office within I&A that is the focal point for DHS support for fusion centers nationwide; and
- trained 12 DHS intelligence officers before they were deployed to state and major urban area fusion centers, as required by the 9/11 Commission Act. The two-hour training session focuses on privacy fundamentals and the DHS FIPPs, information sharing authorities and parameters, data breaches and incident reporting, and intelligence reporting and privacy.

Privacy Support for Fusion Centers

All 71 officially designated state and major urban area fusion centers now have written privacy policies that are at least as comprehensive as the ISE Guidelines.

In collaboration with CRCL, the PISI Group:

- conducted an additional Train-the-Trainer session for newly appointed fusion center privacy officers who were unable to attend prior regional Train-the-Trainer sessions as described in last year's Annual Report.[20] New privacy officers from 12 fusion centers participated. PISI staff provided additional assistance upon request when fusion center privacy officers crafted their own locally-focused fusion center privacy training;
- provided on-site training with CRCL for 15 fusion centers in California, Delaware, Indiana, Mississippi, Nebraska, New Jersey, North Carolina, Ohio, Oklahoma, and South Carolina, to complement the comprehensive, state-specific training delivered by each fusion center's privacy officials. Additional in-person training sessions are planned at six more centers during the remainder of calendar year 2011;
- published a web-based Toolkit, a single source of information and useful resources about fusion center privacy and civil liberties protections that privacy officials and intelligence analysts can use to understand and enhance privacy in their operations. The Toolkit is updated regularly and available online at http://www.it.ojp.gov/privacyliberty; and
- participated in the National Fusion Center Conference for the fourth consecutive year. The DHS Chief Privacy Officer participated on a panel, *Building a Fusion Center Culture that Shares Information While Protecting Privacy and Civil Liberties*, where she stressed the importance of implementing the commitments expressed in each fusion center's privacy policy. PISI also briefed Fusion Center Directors on the DHS Privacy Office's review of fusion center privacy policies, staffed a hands-on learning lab, and hosted an information booth with CRCL to answer attendees' questions.

[20] The 2010 Annual Report is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf.

The DHS Privacy Office will continue to review policies submitted by fusion center nodes, which usually have a regional focus and a relationship to one of the 71officially designated fusion centers. Through June 30, 2011, the DHS Chief Privacy Officer approved 10 policies covering fusion center nodes.

Also during this reporting period the PISI Group:

- continued reviewing intelligence reports and products for privacy related issues before release to the intelligence community and state and local stakeholders. During this reporting year, the PISI Group reviewed approximately 270 analytical products and 310 Homeland Intelligence Reports (HIRs).[21] I&A analysts continually improved in incorporating privacy principles in reports and products, and now the DHS Privacy Office clears approximately 80 % of all HIRs and 70 % of all products upon first review; and
- briefed I&A staff on the DHS Privacy Office's role in I&A product reviews at a Town Hall meeting in March 2011, and in other fora. The Office's review of HIRs and intelligence products will continue to strengthen the quality of DHS intelligence products and enhance integration of privacy protections.

[21] HIRs contain "raw" intelligence information that is shared within the Intelligence Community and state and local partners for informational purposes. The information has not been evaluated or analyzed.

V. Privacy in Technology

The intersection of privacy and technology requires the DHS Privacy Office to provide specialized guidance to DHS components to support the Department's development of new technologies. During this reporting period, the Privacy Technology Group (Technology Group) focused on cybersecurity, the Federal Open Government Initiative, cloud computing, and public awareness. Highlights of each of those focus areas are detailed below.

A. Cybersecurity

The DHS Privacy Office collaborated with the DHS National Protection and Programs Directorate (NPPD) Office of Privacy to further integrate privacy protections into the Department's cybersecurity activities and foster greater transparency and oversight. During the reporting period, the Technology Group:

- initiated an assessment of the Department's National Cybersecurity Protection System and collaborated with the Compliance Group and the National Protection and Programs Directorate (NPPD) Office of Privacy to develop a strategy for assessing the privacy impacts of the Department's overall cybersecurity program;
- staffed DHS's new Office of Cybersecurity Coordination located at the National Security Agency (NSA). The DHS Privacy Office onsite staff at the NSA address privacy issues related to the work of this new coordination office and strengthen collaborative relationships with onsite NSA and Department of Defense (DoD) colleagues;
- facilitated three classified briefings on the EINSTEIN program for the DHS Data Privacy and Integrity Advisory Committee (DPIAC) Cybersecurity Subcommittee; and
- issued, in June 2011, a new Privacy Policy Guidance Memorandum entitled *Roles & Responsibilities for Shared IT Services*,[22] signed by the Chief Privacy Officer, the Chief Information Officer (CIO), the Assistant Secretary for Policy, and the Director of Records. Sharable technology enables the Department to focus its efforts on building a single version of a particular system and reuse that system across all components. This new policy clarifies the roles and responsibilities of components sharing IT services, requiring, for example, that a single component will be responsible for ensuring all uses of a particular data set are appropriate across all users of the shared IT service.

[22] https://www.dhs.gov/xlibrary/assets/privacy/dhsprivacy-policyguidancememorandum-2011-02.pdf.

B. Open Government Initiative

In December 2009, OMB issued an *Open Government Directive* requiring federal executive departments and agencies to increase transparency, public participation, and collaboration in government.[23] Since then, the DHS Privacy Office has played a leading role in the Department's compliance with the *Open Government Directive* by conducting privacy reviews of data sets to be posted on the data.gov and USAspending.gov websites. The Technology Group, together with the FOIA staff in the Office, ensures the data sets DHS proposes comply with DHS policy, privacy laws, regulations, and OMB guidance before they are posted. The Office reviewed a total of 57 data sets, including FOIA logs and FEMA disaster summaries, for potential privacy concerns.

C. Cloud Computing

In September 2009, the Federal Chief Information Officer announced a new initiative to save money and time by transferring government information systems to cloud computing.[24] The Technology Group has been actively involved in this initiative from the beginning. During this reporting year, the Technology Group:

- contributed to the Federal CIO Council Privacy Committee's Web 2.0 Subcommittee's paper, *Privacy Recommendations for the Use of Cloud Computing by Federal Departments and Agencies.*[25] This paper identifies privacy risks associated with cloud computing and details good privacy practices for the transition to cloud computing;
- continued to be actively engaged in the Federal CIO Council's FedRAMP (Federal Risk and Authorization Management Program) process to ensure privacy is considered throughout the planning and implementation stages of cloud computing, and participated in tiger teams regarding privacy and other issues posed by the government's use of cloud computing; and
- participated in a new inter-agency group of IT, legal, procurement and privacy personnel convened to ensure the government analyzes cloud computing in depth.

[23] Office of Mgmt. & Budget, Executive Office of the President, OMB Memorandum No. M-10-06, *Open Government Directive* (2009), available at http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-06.pdf.
[24] Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. More information is available at http://www.whitehouse.gov/blog/Streaming-at-100-In-the-Cloud/.
[25] The paper is available at http://www.cio.gov/Documents/Privacy-Recommendations-Cloud-Computing-8-19-2010.docx

VI. Collaboration Within and Outside DHS

The DHS Privacy Office engages with many individuals, groups, and agencies both inside and outside of the Department. The Office has been increasingly active on an inter-agency basis to help embed privacy requirements in a number of documents that will be utilized across the federal government. Highlights of the Office's efforts inside and outside of the Department are discussed in the following sections.

A. Collaboration within DHS

During this reporting period, the Office:

- issued a report, in collaboration with CRCL and U.S. Customs and Border Protection (CBP) Privacy staff,[26] recommending enhancements to the training that CBP Office of Field Operations officers receive regarding searches of electronic devices at U.S. borders;[27]
- co-hosted a booth and learning lab with CRCL at the March 2011 National Fusion Center Conference;
- collaborated with the U.S. Citizenship and Immigration Services (USCIS) Privacy Officer to create a customized factsheet for the USCIS Vermont Service Center. The Office also provided the customizable fact sheet to component privacy offices for tailoring to address each component's unique privacy issues and to disseminate via intranet sites, staff meetings, privacy trainings, and privacy awareness events;
- participated on the newly formed DHS Identity, Credential, and Access Management (ICAM) Executive Steering Committee (ESC), with the Chief Privacy Officer as a voting member. The ESC is co-chaired by the DHS CIO and the DHS Chief Security Officer. The ICAM ESC is the Department's core oversight and advisory body for ensuring implementation of the Department's ICAM program and related projects and initiatives;
- held bi-weekly teleconferences with CRCL to discuss issues of common concern, and worked closely in support of the national network of fusion centers. Conducted training for fusion center staff and DHS intelligence officers at those centers. This training is discussed in further detail in Part One, Section IV.C of this report;
- participated in bi-weekly DHS CIO Council meetings and in meetings of the CISO Council Security Policy Working Group. The Office gained a better understanding of

[26] See pages 13-14, 40 of the 2010 Annual Report, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf.
[27] The report, entitled *U.S. Customs and Border Protection Border Search of Electronic Devices Containing Information Training: Assessment and Recommendations* (August 20, 2010), is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy-report-cbp-training-border-searches-electronic-devices.pdf.

systems being considered for development, planned and proposed changes to existing systems, systems being retired, and updates to information security policies and procedures that could impact privacy (e.g., updates and changes to *DHS Directive 4300A* and *DHS 4300A Handbook*);

- reviewed and provided comments to CISO on documents that impact privacy, including the CISO's Computer Readable Extract guidance, and the Social Media Policy; and
- worked closely with its cybersecurity colleagues across the Department to identify and address privacy policy and compliance requirements for DHS cybersecurity activities. As DHS's cybersecurity programs connect with and support other federal departments and federal agencies, the DHS Privacy Office also offers its support to those departments and agencies as they conduct their privacy impact assessments of their cybersecurity programs.

B. Collaboration within the Federal Government

The Chief Privacy Officer serves as co-chair of the Federal CIO Council[28] Privacy Committee, the organization of federal senior agency officials for privacy and chief privacy officers. DHS Privacy Office staff serve as co-chairs of the Privacy Committee's Best Practices and Identity Management Subcommittees. The Privacy Office staff:

- co-chaired the Privacy Committee's Best Practices Subcommittee with the Federal Deposit Insurance Corporation. The Subcommittee continued its work on several projects intended to further privacy protections throughout the federal government, including draft privacy controls to appear in an appendix to NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*;[29]
- co-chaired the Identity Management (IdM) Subcommittee with the Federal Trade Commission (FTC). The IdM Subcommittee has been an active contributor this year to numerous "Open Government" initiatives, particularly relating to the development of the *Federal Identity, Credential and Access Management Roadmap and Implementation Guidance (FICAM Roadmap)*;
- assisted in planning the Committee's Privacy Summit hosted for all federal privacy professionals in October 2010. Several privacy office staff served on panels during the summit, which included a full day of training sessions and presentations about federal privacy practices;
- continued to make significant contributions to the Committee's International Privacy Subcommittee. The Subcommittee is a valuable forum for staying apprised of international privacy initiatives throughout the federal government and helps to ensure a consistent message among the many multilateral fora; and

[28] The Federal CIO Council was first established by Executive Order in 1996 and codified into law by Congress in the E-Government Act of 2002. *See* the CIO Council website at http://www.cio.gov/pages.cfm/page/About-Us.
[29] As noted in Part One, Section II, in the summer NIST sought public comment on NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (proposed name change), Draft Appendix J, Privacy Control Catalog, available at http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf.

- participated on the Committee's Web 2.0 Subcommittee to develop government-wide social media SORN and PIA templates and the Privacy Committee's guidance for federal agency use.

In addition, the DHS Privacy Office staff:

- enhanced coordination among public and private sector entities for State Department-hosted international visitor programs; and
- expanded the Office's participation in the Federal CIO Council ICAM initiatives, including the *FICAM Roadmap*. The Roadmap audience includes the federal government, local and state agencies, and private businesses. The DHS Privacy Office's Director of Privacy Policy has been actively participating as a member of the "Roadmap Development Team," which is drafting the implementation chapters of the FICAM Roadmap.

VII. DHS Training and Education

The DHS Privacy Office collaborates with other Department offices and components to develop mandatory privacy training for all employees and contractors, and to include privacy themes in supplemental training classes. The Office also supports targeted training efforts such as training provided by component privacy offices and privacy training for fusion centers. Additional information on these trainings can be found in Appendix II.D.

The DHS Privacy Office continued to execute its ongoing responsibility to ensure that DHS personnel understand the privacy implications of their daily work and handle PII responsibly in accordance with the Privacy Act and DHS Privacy Office guidance. To that end, the Office utilizes mandatory, supplemental, and compliance training to ensure all DHS employees and contractors adhere to privacy related laws and regulations, as well as DHS specific policies. Accomplishments and highlights from this reporting period are included below.

- Mandatory privacy training: 92% of all departmental staff completed the annual training requirement during this reporting period. As noted in Part One, Section II of this Report, the DHS Privacy Office is developing a new online course for all staff, which will include case studies to train staff on the proper methods of safeguarding Sensitive PII.
- New employee privacy training: DHS Headquarters staff receive two privacy overview courses in a classroom setting within six months of hire.
- Job-specific privacy training: USCIS and U.S. Immigration and Customs Enforcement (ICE) developed, and the DHS Privacy Office reviewed, comprehensive role-based privacy training courses this year targeting staff handling Sensitive PII. The Office is working with other components to develop similar training programs.
- International attaché privacy training: The DHS Privacy Office is creating a new web-based course to raise awareness among DHS international attachés and liaisons on U.S. privacy laws and DHS privacy policies in a foreign policy context. More information on this training is in Part Three, Section B.
- New training aid: During all classroom training, the DHS Privacy Office distributes a two-page factsheet detailing best practices for safeguarding Sensitive PII (shown at right).


Homeland Security

HOW TO SAFEGUARD PERSONALLY IDENTIFIABLE INFORMATION

- New intranet site: The DHS Privacy Office launched a new intranet site featuring the Office's privacy and FOIA training resources to raise awareness of the Office's educational programs internally.

VIII. Highlights of Component Privacy Programs and Initiatives

Component privacy officers serve as first-line authorities on privacy issues related to their components' collection and use of PII. They are a critical part of operational privacy efforts across DHS, and are responsible for the day-to-day privacy policy, training, and compliance activities within their respective components. During the past several years, these component privacy programs have grown significantly, particularly because of the Deputy Secretary's June 5, 2009 instruction to components discussed in the 2009 Annual Report.[30] This section highlights their activities during this reporting period.

A. CBP

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 PII for a variety of border security, trade compliance, and law enforcement purposes. The CBP Privacy Office has an integral part in ensuring the proper use of PII.

During the reporting period, the CBP Privacy Office:

- published a PIA on TECS, which is both an information-sharing platform that allows users to access different databases that may be maintained on the platform or accessed through the platform, and the name of a system of records that includes temporary and permanent enforcement, inspection, and operational records relevant to the antiterrorism and law enforcement mission of CBP and numerous other federal agencies that it supports. The PIA discusses the privacy risks and the safeguards that mitigate those risks with regard to the collection of information from the travelling public maintained in TECS;[31];
- devoted significant resources to overseeing proper information sharing with other federal, state, and local government agencies. This role ensures that shared information will be used in a manner consistent with the purpose described in a particular system's PIA and SORN;
- reviewed over 400 one-time information requests, issuing an authorization memorandum specific to each case. Although the number of individual requests remains high, the decrease from the 450 requests during the last reporting period may reflect an increase in the use of memoranda of agreement for recurring information sharing; and

[30] The DHS Privacy Office's 2009 Annual Report is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf.
[31] The PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_tecs.pdf.

- expanded the membership within the Commercial Targeting and Analysis Center (CTAC) by a multiagency Memorandum of Understanding (MOU) with ICE, the U.S. Department of Agriculture's Animal and Plant Health Inspection Service and Food Safety Inspection Service, and the U.S. Consumer Product Safety Commission. CBP's Privacy Office led drafting and negotiation of the MOU; the Commissioner of Customs and leadership of other agencies signed the MOU. At the CTAC, these agencies will share and analyze important data collected by CBP and the participating agencies to enhance their collective and individual abilities to interdict unsafe and harmful imports.

B. FEMA

FEMA's mission is to support the public and first responders to ensure that our nation works together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

During the reporting period, FEMA's Privacy Program increased its effectiveness and impact in the following areas and ways:

1. Leadership, Policy, and Administration

- Reduced the Vulnerability of FEMA's Data to Identity Theft - In October 2010, FEMA's Administrator initiated an effort to reduce the vulnerability of FEMA's data to identity theft, specifically focusing on reducing the agency's collection and use of Social Security Numbers (SSNs). The FEMA Privacy Officer worked with FEMA's Chief Administrative Officer, Chief Information Officer, and Office of Chief Counsel to conduct a comprehensive review of FEMA's systems, forms, and programs that collect SSNs to ensure FEMA is collecting SSNs only when and where necessary. As a result of the analysis, SSNs are collected less frequently, and FEMA is using the initiative to ensure that the relevant privacy compliance documentation is complete and current.
- FEMA Privacy Office Implemented Privacy Office Tracking System (POTS) - Implemented a POTS to track activities related to privacy compliance, policy, training, and incident response, and administrative responsibilities. FEMA can use POTS to track and report programmatic privacy accomplishments.

2. Compliance

- Increased FISMA related privacy scores for PIAs from 48% to 80%, and from 94% to 97% for SORNs.
- Completed 3 PIAs, 2 SORNs and 39 PTAs during the reporting year.
- Published a Notice of Proposed Rulemaking concerning FEMA training and exercise programs in April 2011, and the Final Rule in June 2011.

3. Privacy Incidents, Responses and Mitigation

FEMA continued its efforts to increase privacy awareness and reduce privacy incidents. FEMA's efforts, such as its full deployment of new laptops with encryption software, its increased in-person training efforts, risk analyses, and site visits have contributed to a decrease in privacy incidents at FEMA in the last year. As a result, FEMA has one of the lower percentages

of open privacy incidents in the Department. In addition, the FEMA Privacy Office did not receive any privacy-related complaints during this reporting period.

4. Training and Outreach Activities

- Conducted weekly privacy awareness training for new employees during the Enter-On-Duty Orientation and new contractors during the New Contractors Orientation. Additionally, the FEMA Privacy Office provided privacy reference materials via welcome e-mails to new FEMA employees regarding future privacy awareness and training efforts.

FEMA Privacy Training

The FEMA Privacy Office trained 3,786 employees and contractors nationwide during the reporting period.

- Provided training to four FEMA regions and three National Processing Service Centers either in person or via teleconference.
- Continued to develop a web-based training initiative to make privacy awareness training available to all FEMA employees. The course will be available to employees and contractors through the FEMA Emergency Management Institute's Learning Management System.
- Conducted a site visit and risk analysis of physical space at FEMA's Office of Occupational Safety, Health, and Environment to address privacy-related concerns and offer personnel guidance for safeguarding information in the course of their duties.

C. I&A

I&A's primary goal is to provide intelligence support across the full range of Homeland Security missions. I&A ensures that information related to homeland security threats is collected, analyzed, and disseminated to all relevant customers. In support of that mission, the I&A Privacy Office now has a full-time Privacy Officer and continues to execute its Privacy Development Strategy under its new leadership. During this reporting year, the I&A Privacy Office focused on developing privacy guidance, assessing I&A directorates to identify gaps and mitigate risks with regards to privacy, and enhancing its administrative capabilities. To help embed privacy into all I&A activities, the I&A Privacy Office:

- developed privacy guidance (including procedures to formalize sustainable privacy processes across I&A), Sensitive PII handling procedures, and an encryption white paper outlining the need to encrypt emails containing PII;
- partnered with I&A directorates to identify and mitigate privacy risks across I&A. For example, in coordination with three of the five I&A directorates (Analysis; Enterprise and Mission Support; and Plans, Policy and Performance Management) the I&A Privacy Office conducted privacy gap assessments to identify privacy risks, and facilitated numerous privacy compliance documents to mitigate gaps and risks identified during the assessments; and
- developed capability in support of I&A privacy administration to provide better accounting, processes, and repeatable procedures related to privacy for all I&A staff. Highlights include: developing I&A SharePoint Site content to enhance the

organization's knowledge management capacity by providing common access to privacy tools, processes and procedures.

D. ICE

ICE is the principal investigative arm of DHS and the second largest investigative agency in the federal government. ICE now has more than 20,000 employees in offices in all 50 states and 48 foreign countries. ICE's primary mission is to promote homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration.

ICE deployed a Privacy Act Disclosure Tool via its intranet website that guides employees through a question-and-answer process to help them determine if the Privacy Act authorizes disclosure of a particular record about an individual to a recipient outside of DHS. This tool is an adjunct to the two-hour intensive privacy training the ICE Privacy Office began delivering in 2010, which trains on Privacy Act disclosure rules using real-life scenarios.

In this reporting year, ICE integrated privacy protections into the design of SharePoint collaboration intranet sites deployed on the ICE network. These sites are a repository for shared calendars, bulletin boards, Internet links, and documents for ICE offices, units, project teams, and working groups. The ICE Privacy Office established safeguards to minimize privacy risks on these sites including:

- designating sites as either authorized or not authorized to contain Sensitive PII;
- establishing visual cues, such as different background colors and warning banners, to help users distinguish between sites authorized for Sensitive PII and those that are not;
- limiting access to sites authorized for Sensitive PII to only those with a need-to-know;
- displaying instructions for users detailing what to do if Sensitive PII is inappropriately posted to a site;
- providing special training to site administrators about privacy requirements and their obligation to monitor access controls and content;
- requiring all ICE personnel to complete mandatory online training about these privacy controls; and
- conducting periodic site reviews to ensure compliance.

As evidence of the success of these safeguards, the DHS CIO adopted most of the ICE safeguards in Department-wide SharePoint sites. ICE commenced internal compliance reviews of these sites in May 2011.

For the first time, ICE included privacy performance goals in the Performance Work Plan for supervisors across the agency in Fiscal Year 2011. The goals set minimum performance standards for supervisors on privacy. For example, to "achieve expectations" for the privacy goal, supervisors must ensure their employees complete mandatory privacy and security training, review the *SPII Handbook*, and are periodically reminded about the requirement to report privacy and security incidents. Higher performance standards were established for supervisors to receive a rating of "achieved excellence" for the privacy goal.

In April 2011, ICE implemented a new process to improve the security and privacy of live PII that ICE uses to test ICE IT networks, systems, or tools before deployment. The ICE Privacy Office worked with ICE's CISO to design a questionnaire for any proposal to use live PII in an IT testing process. ICE uses the questionnaire to determine whether there are feasible alternatives (e.g., synthetic data or de-identification) to using live PII and to mitigate security and privacy risks associated with the proposal. The questionnaire was included in the ICE System Lifecycle Management process. ICE Privacy Officer and CISO approval is required before testing with live PII may occur.

During the reporting period, ICE completed 11 PIAs or PIA updates in compliance with the E-Government Act.

E. NPPD

NPPD's goal is to advance the Department's risk-reduction mission. Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements. The NPPD Office of Privacy was established in August 2010 with the hiring of the Senior Privacy Officer, who is charged with integrating privacy into the NPPD mission.

Prior to the establishment of the NPPD Office of Privacy, the DHS Privacy Office oversaw much of NPPD's privacy compliance work, with the exception of the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, whose privacy program pre-dates the establishment of the NPPD Office of Privacy. The DHS Privacy Office was instrumental in overseeing NPPD's privacy compliance efforts, and the Office provided temporary resources to NPPD. The Office's support of NPPD helped embed privacy throughout NPPD. Since August 2010, the NPPD Office of Privacy has had direct responsibility for the integration of privacy policies in all offices of NPPD. More information about NPPD and US-VISIT is included in Appendix III.A.

1. Compliance Activities

During the reporting period, NPPD's Office of Privacy conducted several programmatic and system-based PIAs and SORNs.

- Published a PIA to reflect NPPD's activities under the National Infrastructure Coordinating Center (NICC) SAR Initiative. The NICC SAR Initiative serves as a mechanism by which a report involving suspicious behavior related to an observed encounter or reported activity is received and evaluated to determine its potential nexus to terrorism. As described in Part One, Section I, this PIA is part of the Department-wide process for systematizing how DHS handles SARs, and specifically SARs that meets the National ISE-SAR Initiative Functional Standard 1.5. The Office of Privacy also published a SORN for the NICC SAR Initiative.
- Recertified its PIA for the Critical Infrastructure Warning Information Network (CWIN). The mission of CWIN is to facilitate immediate alert, notification, sharing and collaboration of critical infrastructure and cyber information within and between Government and industry partners.
- Published its PIA for the Chemical Facility Anti-Terrorism Standards Personnel Surety (CFATS PS) Program to assess the privacy impact to individuals affected by the

program.[32] The CFATS PS Program allows chemical facilities to comply with Risk Based Performance Standards (RBPS)-12 by implementing "measures designed to identify people with terrorist ties."[33] The Office also published a SORN for CFATS PS.

2. Privacy in Technology

Technology is growing rapidly, and NPPD is at the forefront of development of technology to assist in the protection of the Nation's critical infrastructure and key resources. NPPD's Office of Privacy works to incorporate FIPPs into new technological developments and programs that utilize technology in ways that affect PII. During this reporting period, NPPD's Office of Privacy:

- worked to embed privacy into the technologies being utilized for cyber detection and to mitigate the risks associated with securing our Nation's infrastructure from cyber attacks;
- participated in a privacy compliance review of the EINSTEIN Program conducted by the DHS Privacy Office's Director of Privacy Compliance; and
- worked closely with NPPD's *Stop. Think. Connect.* campaign to ensure that social media practices include adequate privacy protections.[34]

3. Collaboration Within and Outside DHS

The NPPD Office of Privacy and US-VISIT Privacy Office were extensively involved in ensuring that NPPD's programs worked with internal and external partners to incorporate privacy protections into outreach activities and information sharing agreements. During this reporting period:

- the NPPD Office of Privacy reviewed and provided advice on six Closed Circuit Television (CCTV) privacy policies for organizations within the City of Philadelphia, as required by DHS and the City of Philadelphia CCTV Grant Terms and Conditions;
- US-VISIT hosted three members of the Unique Identification Authority of India (UIDAI). UIDAI is an agency of the Government of India responsible for implementing the envisioned Multipurpose National Identity Card or Unique Identification card (UID Card) project in India. The Privacy team participated by presenting a briefing on US-VISIT data protection and the redress process; and
- US-VISIT hosted a Republic of Korea delegation as part of information sharing efforts under the two countries' Enhancing Cooperation to Prevent and Combat Serious Crime Agreement signed on November 7, 2008. US-VISIT's Privacy team participated in discussions with the delegation and presented a briefing about US-VISIT's privacy policies and redress process.

[32] On October 4, 2006, the President signed the Department of Homeland Security Appropriations Act of 2007 (the Act), Public Law 109-295. Section 550 of the Act (Section 550) provides DHS with the authority to regulate the security of high-risk chemical facilities. DHS has promulgated regulations implementing Section 550, the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR Part 27.

[33] Section 550 requires that DHS establish RBPS as part of CFATS. RBPS-12 (6 CFR 27.230(a)(12)(iv)).

[34] The *Stop. Think. Connect.* campaign is a national public awareness effort to guide the nation to a higher level of Internet safety by challenging the American public to be more vigilant about developing safe online habits. The campaign utilized social media to disseminate information and engage the public to participate in its programs.

4. Training and Education

During this reporting period, NPPD began implementing a communications plan to increase awareness of privacy both within and outside the Department. The plan included:

- privacy briefings for new NPPD employees when they enter on duty;
- specialized privacy training for all US-VISIT federal employees and contractors before granting access to agency information and information systems;[35]
- mandatory DHS Privacy Office's *A Culture of Privacy Awareness* course for all NPPD employees;
- in October 2010, over 200 US-VISIT employees and contractors, and other DHS employees attended US-VISIT's third annual Privacy Awareness Week. Experts from DHS and other federal agencies conducted presentations on identity theft, consumer fraud, international privacy issues, and health information technology. Privacy and data protection posters were displayed throughout US-VISIT's office spaces and remain on display to remind personnel of the importance of privacy and data protection at US-VISIT; and
- both the NPPD and US-VISIT privacy programs also provide ad hoc and role-based training for NPPD staff throughout the year. During the reporting period:
    - the NPPD Senior Privacy Officer and the DHS Privacy Office's Associate Director for Compliance conducted in-person training to 20 Infrastructure Protection employees and contractors;
    - NPPD Senior Privacy Officer conducted training for 14 Federal Protective Service Field agents;
    - NPPD held role-based privacy training for its field Site Security Officers;
    - approximately 2,307 NPPD federal employees, including US-VISIT employees, completed the *A Culture of Privacy Awareness* course;
    - 499 new NPPD employees completed a privacy briefing given during the new employee orientation.

NPPD conducted other privacy awareness activities on topics including PII, FOIA, and PIAs as discussed in Appendix III.A.

F. S&T

The Science & Technology Directorate (S&T) was established by the Homeland Security Act of 2002. S&T advises the DHS Secretary on research and development issues; implements a national plan to identify and develop counter measures to chemical, biological, and other emerging terrorist threats; and conducts basic and applied research, development, demonstration, testing, and evaluation activities that are relevant to any or all elements of the Department, through both intramural and extramural programs.

[35] http://www.dhs.gov/files/programs/usv.shtm.

S&T manages, oversees, or conducts more than 120 projects in areas such as: borders and maritime security; chemical and biological defense; cybersecurity; explosives; human factors and behavioral sciences; and infrastructure protection and disaster management.

During this reporting period, S&T achieved several significant milestones. S&T hired its first Privacy Officer, who continues to build privacy into all S&T projects by following the Privacy by Design philosophy. The two objectives of the philosophy are to integrate privacy into the lifecycle of projects, particularly in early initial concept phases, and to create opportunities for program managers to achieve program goals, while respecting privacy rights. During this reporting period, the S&T Privacy Office:

- obtained approval for a new Information Lifecycle Management Office to create a "one-stop shop" for information and guidance by bringing together privacy, FOIA, and other data management functions;
- achieved 100% compliance on the Trusted Agent FISMA Privacy Report by completing PIAs and SORNs for all S&T operational systems collecting PII;
- published a PIA for the Cell All Program, which is a project at the Homeland Security Advanced Research Projects Agency involving the research and development of a personal environmental threat detector system using a typical cell phone platform. This PIA identifies privacy sensitivities and risks associated with mobile applications;
- published an umbrella Volunteers PIA to streamline compliance process for projects involving research volunteers. Thirty-five research projects that involve volunteer participants and are in privacy compliance have used this PIA instead of writing separate PIAs. Completing the Volunteers PIA addressed privacy protections such as informed consent forms for research projects involving volunteer participants. The PIA also addressed blurring facial photographs and anonymizing aggregated data. More information on this PIA is included in Appendix III.B;
- finalized a Virtual USA Principles document that is distributed to state and local emergency responders using the Virtual USA system. Understanding that each state has its own privacy laws and regulations, S&T created these Principles to provide guidance on the Department's privacy policies;[36] and
- conducted the Iris and Face Technology Demonstration and Evaluation test program. DHS S&T and NIST are investigating iris recognition as a promising biometric modality that may become suitable to support DHS operations in the near future.[37]

The S&T Privacy Office worked on numerous PTAs, PIAs and SORNs on a wide range of issues (e.g., cybersecurity, biodefense, and research data collection issues). Information on these efforts is included in Appendix III.B.

[36] The Virtual USA Principles are available at https://vusa.us/resources.html.

[37] The purpose of this evaluation of iris recognition technologies is to conduct field trials/studies of iris camera prototypes under conditions and environments of relevance (e.g., humidity levels, amount of sunlight, etc.) in collaboration with CBP to assess the viability of the technology and its potential operational effectiveness in support of DHS operations.

G. Transportation Security Administration

The Transportation Security Administration (TSA) is responsible for protecting the nation's transportation systems to ensure freedom of movement for people and commerce. In addition to its aviation security efforts, TSA also works with public and private partners to enhance security of other modes of transporting people and commodities including highways, maritime ports, rail, mass transit, and pipelines.

The TSA Office of Privacy Policy and Compliance seeks to address privacy matters affecting travelers, transportation sector workers, and TSA personnel by providing guidance to programs, responding to inquiries, performing outreach, and assisting with legal compliance.

1. Outreach and Awareness

With over 50,000 employees at more than 460 locations, TSA privacy awareness efforts are a continuing significant commitment. During the reporting period, the TSA Office of Privacy Policy and Compliance:

- maintained privacy awareness across the employee and contractor work force by using "TSA TV," space available on hard-copy Leave and Earnings Statements, and by broadcasting email on topics including how to protect Sensitive PII, and accessing data for official purposes;
- collaborated with the Office of the Chief Information Officer's communications team to develop data security messages;
- presented at employee training events (e.g., Intelligence Office and Information System Security Officer training), maintained an internal website with privacy resources for TSA employees and issued the "Privacy Awareness Press" series to sensitize program managers on privacy issues that received media attention;
- presented at fora outside of DHS, including the CIO Council Federal Privacy Summit (on PII protection requirements in contracting), the Department of Veterans Affairs (on social media), and at an International Association of Privacy Professionals (IAPP) conference;
- met with outside stakeholders including representatives from privacy, religious, and transgender groups, and international officials, on Advanced Imaging Technology (AIT) activities;
- published or updated eight PIAs as listed in Appendix II; and
- reviewed more than 400 IT proposed acquisition statements of work to evaluate privacy impacts and PII protection clauses.

2. Programs

The use of AIT, which safely screens passengers for metallic and non-metallic threats, including weapons, explosives and other objects concealed under layers of clothing, is a program with continued public interest, as discussed in the DHS Privacy Office's 2009 and 2010 Annual Reports.[38] During this reporting period, TSA piloted Automated Target Recognition (ATR) imaging functions that effectively recognize anomalies and thereby eliminate the need for an operator to view the actual body image created by existing technology. TSA expects ATR to address concerns among those passengers who raise modesty objections about the viewing of existing AIT images by a remotely located operator.

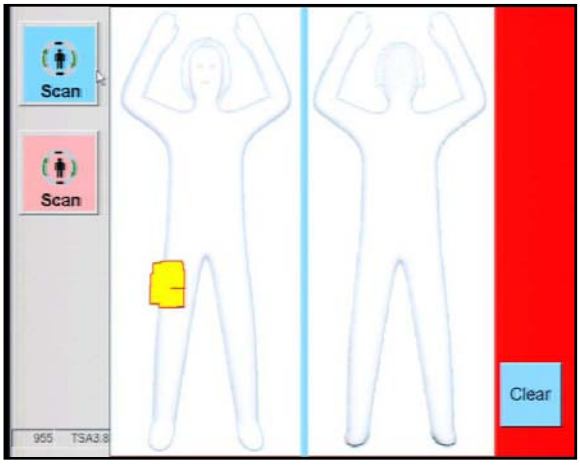


Figure 6: ATR Body Scan Image

TSA also launched *MyTSA*, a free mobile application for members of the public seeking information (e.g., items permitted through security, items that can be carried in checked baggage) on air travel. *MyTSA* permits members of the public to share security checkpoint wait times to make use of a data feed provided by the FAA regarding airport delays due to weather or other factors. *MyTSA* does not collect or use PII. It permits the use of the GPS features of the mobile device to highlight local information, but will allow the user to input any location to search for information about that location. *MyTSA* does not transmit location information to TSA. TSA published a PIA for *MyTSA* on July 1, 2010.[39] In March 2011, the American Council for Technology-Industry Advisory Council recognized the *MyTSA* application as a Best Government Mobile App.

H. USCG

The U.S. Coast Guard (USCG) Privacy Program is located in the Office of Information Management, a division of the Assistant Commandant for Command, Control, Communications, Computers and Information Technology CIO Directorate. The Office of Information Management is an integral component of the CIO organization, managing FOIA and Privacy Act, Postal, Records, Forms, E-Government, Directives and Publications, Printing, Correspondence, and Information Collections programs. The Privacy Program is responsible for the promulgation and interpretation of privacy policy, compliance documentation, incident/compliance management, myriad reporting requirements, training, and related directives policy review. In June 2011, USCG welcomed a new Coast Guard Privacy Officer.

During this reporting period, the Privacy Program:

- conducted biennial review of 21 SORNs;

[38] See page 55 of the 2010 Annual Report, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf; See page 59 of the 2009 Annual Report, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf.
[39] Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_mytsa.pdf.

- obtained approval for College Board Recruitment Plus and Merchant Mariner Licensing & Documentation System PIAs and updated the Biometrics at Sea PIA during triennial review;
- achieved privacy compliance for programs including SAR, the National Recreational Boating Survey, and Social Media, consistent with Department-wide standards;
- responded and collaborated with agency-wide staff on privacy incidents, ensuring remediation measures were established to prevent reoccurrence;
- reviewed over 200 USCG/DHS policy directives to ensure programs, missions, and guidance comply with current federal privacy mandates;
- presented to the DHS Annual Core Management Group meeting on internal incident response and notification processes;[40] and
- presented privacy training at various USCG-sponsored fora (e.g., Annual Privacy Awareness Week, Civil Rights Conference, Servicing Personnel Office Conference).

I. USCIS

USCIS has the responsibility of preserving America's legacy by overseeing lawful immigration to the U.S. and by providing accurate and useful information to its customers, granting immigration and citizenship benefits, promoting awareness and understanding of citizenship, and ensuring the integrity of USCIS' immigration system. In support of that mission, the Office of Privacy works diligently to sustain privacy protections in its programs and initiatives.

The Office of Privacy also strives to enhance the privacy awareness of employees and contractors by developing policies, conducting privacy trainings and outreach opportunities, and participating in working groups.

1. Office of Inspector General Report

Beginning in June 2010, the OIG conducted an audit of USCIS's privacy stewardship to determine if USCIS has established a culture of privacy and if the agency is complying with federal privacy laws and regulations. The audit results released in May 2011[41] identified that USCIS made progress by:

- appointing a privacy officer and establishing the USCIS Office of Privacy;
- monitoring federal privacy laws and regulations to ensure USCIS is and remains compliant;
- providing guidance to managers and employees; and
- conducting privacy trainings.

In addition, the OIG Report identified six recommendations to USCIS; two of the recommendations were privacy-specific. The first recommendation was to identify vulnerabilities and mitigation strategies to reduce the privacy risks associated with Alien Registration Number files by conducting PIAs for high-risk operations at service centers and

[40] See Part One, Section III.A for more information on the CMG.
[41] http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_11-85_May11.pdf

other field activities. The second recommendation was to implement employee suggestions into plans for privacy training and awareness.

During this reporting period, the USCIS Office of Privacy collaborated with several programs to coordinate a response to the OIG's recommendations. In leading the response, the Office of Privacy identified appropriate program office points of contact to address issue items; facilitated group meetings and conference calls to coordinate a response for each issue; compiled, reviewed, and edited draft responses; coordinated with other internal programs to meet milestones and deadlines; and delivered a final response to the USCIS Internal Coordinator for submission to the OIG.

2. Privacy Policy and Guidance

During the reporting period, the USCIS Office of Privacy:

- completed and vetted an internal Breach Memorandum that specifically outlines the responsibilities of USCIS staff when a breach has or may have occurred;
- collaborated with the USCIS Contracting Office to establish an expedited process for notification and credit monitoring following a data breach; and
- disseminated a guidance memorandum prohibiting USCIS staff from including the Alien Registration Numbers on the external mailing label of letters, packages, and boxes.

3. Outreach and Awareness

The USCIS Office of Privacy continued its privacy outreach and awareness initiative by training over 17,000 employees and contractors nationwide during this reporting period. The USCIS Office of Privacy held its first agency-wide annual Privacy Awareness Week. During the week, USCIS hosted the DHS Chief Privacy Officer and speakers from the DHS Privacy Office, United States Secret Service (USSS), FTC, and DOS.

During the reporting period, the USCIS Office of Privacy also:

- conducted bi-weekly trainings for new employees and several trainings specific to the roles and responsibilities of USCIS employees (e.g., the Refugee Asylum and International Staff, Service Center Operations Resource Managers, and Fraud Detection and National Security Analysts and Investigators);
- conducted site visits for training and meetings with staff and the leadership to discuss privacy related issues and concerns;
- worked to finalize a new computer-based privacy awareness training course targeted to the entire USCIS workforce. The training course will be deployed in FY 2012 and will be accessible through USCIS' learning management system;
- developed and conducted multiple training sessions specifically designed for Mission Support Specialists regarding appropriate PII safeguarding and handling; and
- participated in several working groups to ensure privacy is embedded in all new programs and initiatives.

4. Program Offices

a. USCIS Office of Transformation and Coordination

The USCIS Office of Privacy continued to work collaboratively with the Office of Transformation Coordination (OTC), which is responsible for agency-wide organizational and business transformation initiatives, and other key stakeholders, to ensure privacy considerations are embedded throughout the USCIS transformation process. USCIS is transforming paper-based immigration services to an electronic environment. The electronic site will provide improved service, and enhance security and timeliness. In addition, during this reporting period a full time privacy professional was embedded on a long-term detail with OTC to assure privacy protection in each element of the program as it develops.

b. USCIS Verification Division

In March, Secretary Napolitano and USCIS Director Alejandro Mayorkas announced the launch of E-Verify Self Check – an innovative web-based service allowing individuals in the United States to check their employment eligibility status before formally seeking employment. E-Verify Self Check also streamlines the E-Verify process for businesses using E-Verify to confirm an individual's information on the Form I-9.

E-Verify Self Check is a proactive redress tool that serves to protect individual workers' rights and their PII. This voluntary, free and fast service gives users an opportunity to correct errors in their DHS and Social Security Administration records before applying for jobs. Similar to checking their credit, this measure allows U.S. workers to protect themselves from potential workplace discrimination resulting from an employer's abuse of the E-Verify system. The user's information is secure and is not shared with either potential or current employers. USCIS completed a PIA for Self Check during this reporting period.[42]

J. United States Secret Service (USSS)

The USSS 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. In support of that mission, the USSS Privacy Officer undertook several initiatives to continue to promote a culture of privacy awareness and enhance transparency throughout the agency. During the reporting period, the Secret Service:

- required all employees and contractors to successfully complete an annual privacy awareness training course;
- provided instructor-led training to new employees throughout the year on FOIA and the Privacy Act;
- enhanced the USSS intranet page to disseminate information to employees about privacy compliance, guidelines, and tools. The page provides a basic overview of federal privacy laws, including the Privacy Act, FOIA, and the E-Government Act. Privacy compliance guidance materials were posted on the intranet to assist program and project managers in the preparation of PTAs and PIAs, and to meet other privacy compliance requirements;

[42] More information about the E-Verify Self Check PIA is included in Part One, Section I.

- hired a full-time Assistant Privacy Officer to assist the Privacy Officer in the administration and implementation of all privacy statutory and regulatory requirements;
- continued to identify systems requiring PTAs and PIAs through collaboration with USSS Program and/or Project Managers and to review, update, and resubmit expiring Secret Service PTAs;
- reviewed and updated all USSS SORNs as part of the biennial review process to promote transparency;
- presented at the annual DHS Privacy Workshop on privacy compliance issues;
- issued posters, flyers, and an official message distributed to all USSS employees about the importance of safeguarding PII and reporting privacy incidents; and
- established a privacy e-mail account for employees to submit privacy-related questions and comments and notified employees about a dedicated phone line within the FOIA/Privacy Program for privacy and FOIA-related inquiries and comments.

Part Two – Making a Difference: Enhancing Accountability and Transparency

The DHS Privacy Office continues to make a difference by advocating and advancing accountability and transparency of Department operations. Part Two of this Report demonstrates the varied means by which the Office achieved these accomplishments and highlights the leadership role the Office has played both within DHS and across the federal government.

I. Engaging the Public

Since her appointment in March 2009, the Chief Privacy Officer has made engaging the public a primary focus. The Office interacts with the public in a number of ways, many of which directly support the FIPPs in the areas of transparency and individual participation. These activities are critical to maintaining an open dialogue with the public, creating awareness about DHS Privacy Office operations, and reaffirming the Department's commitment to respecting the privacy rights of all people – U.S. citizens, residents, and visitors.

A. Transparency and Disclosure

Transparency, openness, and collaboration are central to the President's and the Attorney General's vision of FOIA. The DHS Privacy Office through its FOIA unit (DHS FOIA Office) coordinates department-level compliance with FOIA through policy development, oversight of component FOIA operations, training, and mandated progress and performance reports. The DHS FOIA Office processes initial FOIA and Privacy Act requests to the Office of the Secretary, including the Military Advisor's Office and the Office of Intergovernmental Affairs, and eight DHS headquarter components, which are collectively referred to as "DHS FOIA Office Components." During this reporting period, the DHS FOIA Office:

- initiated an annual review of DHS FOIA operations;
- formed an action team to encourage and systematize proactive disclosure;
- investigated information technology to better coordinate FOIA across the Department;
- studied the Department's backlog of FOIA requests;
- coordinated the first FOIA workshop for the entire Department; and
- hired a Deputy Chief FOIA Officer at the Senior Executive Service level.

Figure 7: Sunshine Week Poster 1

The DHS FOIA Office leads the charge for the Department in implementing the Obama Administration's commitment to openness and transparency by providing guidance, training, and outreach to DHS offices and components on an ongoing basis. For example, the DHS Chief FOIA Officer:

Operationalizing One DHS FOIA

DHS FOIA reviewed FOIA activities at all components and identified key initiatives to pursue, including identifying and implementing an enterprise-wide electronic solution to manage FOIA cases and significantly increasing DHS records proactively released.

- issued a memorandum to FOIA Officers providing guidance and instructions for making redacted documents compliant with Section 508 of the Rehabilitation Act, or accessible to those with disabilities, before posting them in online FOIA reading rooms;
- created and continues to foster an environment where proactive disclosure is the expected approach through a memorandum[43] requiring the DHS FOIA Office to implement FOIA Subsection (a)(2)(D), which instructs federal agencies to make publicly available substantially the same records requested at least three times over a three-year period;
- posted a combined 11,109 pages from across the Department to the DHS FOIA online library as part of the DHS Privacy Office's proactive disclosure approach; and
- produced and distributed two FOIA-specific posters (Figures 7 and 8) throughout the Department for 2011 Sunshine Week.

The Deputy Chief FOIA Officer undertook a comprehensive review of Department-wide FOIA operations, interviewing component FOIA Officers about the challenges they face on a daily basis. While this multi-pronged inquiry confirmed that the overall state of DHS FOIA operations is sound, indicating that the DHS Privacy Office's efforts to align with the Administration's goals are working, it also identified opportunities to improve the delivery of FOIA services.

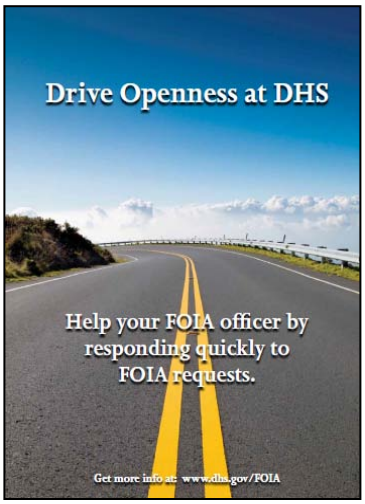


Figure 8: Sunshine Week Poster 2

Training and education are important tools for standardizing FOIA practices and ensuring excellence across DHS. During this reporting period, the DHS FOIA Office:

- convened the first-ever Department-wide FOIA workshop in December 2010. Deputy Secretary Jane Holl Lute emphasized the FOIA commonalities that cut across offices and components and how FOIA supported every element of the Department's mission. She characterized FOIA as central to a transparent and open government and challenged DHS FOIA staff to reach for an even higher level of excellence. Twenty-one FOIA Officers from across the Department spoke at the workshop; and

[43] *DHS FOIA Office Procedures and Standards for Effectively Implementing Section (a)(2)(D) of the FOIA* available at http://www.dhs.gov/xlibrary/assets/foia/cfoiao-memo-dhs-priv-foia-a2d-procedures-20101208.pdf. Documents that have been released proactively are available at the DHS FOIA online library.

- collaborated with the DOJ, Office of Information Policy, to offer in-depth training on the proper application of FOIA Exemption (b)(2) after the United States Supreme Court significantly narrowed the exemption's scope in *Milner v. Department of the Navy*. DHS had historically relied extensively on (b)(2) to protect sensitive information; the *Milner* decision made it necessary to identify alternative means to safeguard information appropriately. The training session addressed concerns specific to DHS and identified ways for DHS offices and components to move forward.

The DHS Privacy Office's commitment to customer service catalyzes the continued expansion of the DHS FOIA online library. DHS FOIA and component FOIA offices have made steady progress toward making the FOIA process more transparent by proactively posting documents released in response to FOIA requests and other documents of public interest, some previously available only by submitting a FOIA request.

DHS FOIA efforts toward that end have been hastened by the formation of a team dedicated to systematically identifying records suitable for proactive release. In addition to enriched library resources, customers will benefit from the reorganization of the DHS FOIA website, which is currently underway.

B. Public Outreach

Throughout this reporting period, the Chief Privacy Officer continued to actively engage the privacy advocacy community in the spirit of openness and transparency, building upon her goal to ensure the advocacy community and privacy stakeholders generally are well informed about DHS programs and projects that may pose particular privacy concerns. Specifically, the Chief Privacy Officer and DHS Privacy Office staff spoke at 32 privacy-related events during this past year. Additional outreach activities are detailed in this section.

1. Privacy Advocacy Community

The Chief Privacy Officer continued to host quarterly Privacy Information for Advocates meetings, a series of informational meetings with members of the advocacy community. During the reporting period, the Chief Privacy Officer also took the initiative to update the privacy advocacy community by email or telephone conference calls about new DHS reports or activities that would be of interest to them.

2. International

The Chief Privacy Officer contributed to the Wilson Center's Canada Institute publication *One Issue Two Voices*, where she discussed privacy and security in border management with a counterpoint author from Canada.[44] During two public events in November in Toronto, Ontario and Washington, D.C., she discussed the U.S. privacy framework and explained how misperceptions of privacy compliance impact U.S.-Canada cooperation.

[44] The issue is available at http://www.wilsoncenter.org/topics/pubs/One%20Issue_13_Privacy.pdf .

3. DHS Blog

During the reporting period, the Chief Privacy Officer was a regular contributor to the DHS Blog (http://blog.dhs.gov).

4. Speaker Series

The DHS Privacy Office is in its fourth year of hosting the DHS Privacy Office Speaker Series. Led by the Privacy Technology Group, the Speaker Series provides an opportunity to host federal and private sector experts for informal discussions with DHS staff on privacy-related topics. During this reporting period, the Office hosted two events.

- A presentation by the Director of the Enterprise Services and Integration Office of the Department of Defense Office of the Chief Information Officer on cost savings, interoperability, culture change, and information sharing related to moving the Department of Defense to cloud computing.
- A presentation by the Assistant General Counsel of the FBI's General Counsel Office, Privacy and Civil Liberties Unit, on the privacy issues raised by the use of DNA in law enforcement investigations.

At the end of the reporting period, the DHS Privacy Office issued its schedule for the 2011-2012 Speaker Series and opened the Series to attendees throughout the federal government. The Office also created a new email address to register for these events, privacyspeakers@dhs.gov, and created a webpage[45] listing each of the upcoming four events through 2012. The Office is initiating a new approach so that the four workshops are thematically organized; the Series began July 2011 and will continue through April 2012. This annual schedule will be built around new and emerging privacy-related topics. The 2012 reporting period Speakers Series will focus on privacy and cybersecurity.

[45] http://www.dhs.gov/files/events/privacy-office-speakers-series.shtm.

II. Complaints and Redress

Efficient responses to privacy complaints and timely resolution of requests for redress are integral to the DHS Privacy Office's core mission.

A. Complaints

The DHS Privacy Office's Director of Privacy Incidents and Inquiries has lead responsibility for reviewing privacy complaints received by the Department. This includes responding to individual complaints as well as overall reporting and monitoring. During the reporting period, the Office:

- reported to Congress through quarterly Section 803 reports that identified the types of complaints received and their disposition;
- monitored the Office's Electronic Complaint Tracking System;
- coordinated with the new DHS Office of Appeals and Redress to measure the effectiveness of redress programs, in particular the DHS Traveler Redress Inquiry Program (DHS TRIP);
- analyzed redress processes throughout DHS; and
- reported annually to the DHS Core Management Group on privacy incident statistics (including incident type, criticality, whether open or closed, and media affected (e.g., laptop, shared drive, thumb drive, compact disk, email, paper, or web posting).

Appendix II.B includes tables that detail on a quarterly basis the categories and disposition of complaints that the DHS Privacy Office received between June 1, 2010 and May 31, 2011.[46]

1. Component Complaint Handling

Collaboration among the DHS Privacy Office and components was a major factor contributing to the successful resolution of the complaints received during this reporting year. One example of a component's handling of a complaint is highlighted below. Additional examples of complaints handled by the components are included in Appendix II.G.

TSA received complaints from individuals who objected to the use of AIT, or objected to any physical screening procedures at airports (more details about AIT are found in Part One, Section VIII.G). TSA responded to complaints by reiterating that the agency adopted privacy safeguards for the use of AIT before the machines were installed, and continues to use comprehensive privacy safeguards in all of its passenger screening methods.

After addressing questions regarding AIT technology, TSA placed the individuals in contact with appropriate TSA staffers capable of addressing physical pat-down concerns. Additionally, TSA

[46] The quarterly reporting period for June 1, 2011 through August 31, 2011 was ongoing at the close of the reporting period for this Report.

directed the individuals to the TSA AIT website, and to ongoing TSA blog discussions addressing specific concerns during this reporting period.

2. Response to Public Inquiries

In addition to complaints, the DHS Privacy Office receives hundreds of email inquiries at privacy@dhs.gov requesting information or providing comments. While most of these inquiries addressed issues outside the area of privacy, the Office made every effort to refer them to the appropriate component or other federal agency for resolution.

B. Redress

Implementing effective redress is another core responsibility of the DHS Privacy Office, and redress may take several forms. Redress for U.S. persons is codified in the Privacy Act. Due to the degree to which DHS interacts with members of the international community, however, the Department has made a policy commitment to provide administrative redress to non-U.S. persons in most of its programs under the DHS Mixed Systems Policy as discussed below.

1. Privacy Act Redress

Under section (d)(2) of the Privacy Act, an individual can request amendment of his or her own record.[47] In February 2011, the Chief Privacy Officer issued *Privacy Policy Guidance Memorandum 2011-01, Privacy Act Amendment Requests*, which sets forth Department policy on identifying, processing, tracking, and reporting on requests for amendment of records submitted to DHS under the Privacy Act of 1974, as amended.[48] During the reporting period, the DHS Privacy Office received no requests for amendment under the Privacy Act. The DHS components and offices received 34 requests. **Table 2** shows requests received by component.

DHS Component	Privacy Act Amendment Requests	Granted	Denied	Pending	No Action Taken[49]
CBP	3	3	0	0	0
ICE	4	2	2	0	0
Management	1	0	1	0	0
NPPD	2	1	1	0	0
OIG	1	0	1	0	0
USCIS	23	8	2	6	7
Total	***34***	***14***	***7***	***6***	***7***

Table 2: Privacy Act Amendment Requests by Component

[47] 5 U.S.C. § 552a(d)(2).
[48] http://www.dhs.gov/xlibrary/assets/privacy/privacy-policy-guidance-memorandum-2011-01.pdf.
[49] USCIS assigns codes to those amendment requests where no action is taken. Those codes with the corresponding number of requests that fall within in the code are: 1) NR – No Record or Non-Possession of Record (1 response); 2) FC – Requestor's Failure to Comply (2 responses); 3) WD – Request was Withdrawn (1 response); 4) NA – Not Applicable or PA Not Applicable (1 response); 5) DP – Duplicate Request (1 response); and 6) RD – Redirected to Another Agency (1 response).

As an example of component offices handling Privacy Act amendment requests, the NPPD Office of Privacy and NPPD FOIA Officer work together to respond to requests for amendment to records maintained within NPPD's records systems. During the reporting period, NPPD received two requests from individuals seeking to have records from NPPD's system of records either expunged or adjusted. NPPD granted a request stemming from a Federal Protective Service (FPS) investigationAn individual requested that NPPD adjust his file as it related to his interactions with the FPS. NPPD agreed to that request by attaching an incident narrative submitted by the individual. Another individual requested that NPPD expunge personnel records. NPPD denied the request because the Federal Government Personnel Records SORN[50] limits access to only determining if the records sought accurately describe the action of the agency ruling on an individual's request. Expunging the personnel record would have erroneously implied that a review of the merits of the action(s) had occurred, thus the denial.

2. Non-Privacy Act Redress

a. Mixed System Policy

As a matter of law, the Privacy Act provides statutory privacy rights to U.S. citizens and Legal Permanent Residents (LPR), collectively known as U.S. persons. As a matter of policy, DHS extends the Privacy Act's protections to non-U.S. persons for information collected, used, retained, and/or disseminated by DHS in mixed systems (i.e., systems that contain information on both U.S. and non-U.S. persons), as set forth in the DHS Privacy Office Privacy Policy Guidance Memorandum *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons (DHS Mixed Systems Policy)*.[51] The DHS Mixed Systems Policy states that any PII collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as if it were subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, LPR, visitor, or alien. Under this policy, DHS handles non-U.S. person PII held in mixed systems in accordance with the DHS FIPPs. The Mixed Systems Policy directly supports the FIPPs principle of individual participation for programs such as the DHS TRIP, which allows for administrative and further judicial redress.

Despite the Mixed Systems Policy, some foreign government officials have questioned whether the U.S. provides effective privacy protections and redress options for their citizens, focusing on the fact that the Privacy Act's protections are limited to U.S. citizens and LPRs. Questions most frequently arise in the context of DHS border protection systems that impact international travelers. During the reporting period, the DHS Privacy Office continued efforts to educate the public, particularly international government officials, on redress options available when individuals believe the Department has inaccurate data or has misused the data held within DHS systems. The Chief Privacy Officer conducted extensive international outreach to raise awareness of the U.S. privacy framework and DHS privacy policy during this reporting period. Part Three, Section II of this Report includes a complete description of these outreach activities.

[50] Federal Register Vol. 71, No. 117, at 35342, available at http://www.gpo.gov/fdsys/pkg/FR-2006-06-19/pdf/06-5459.pdf.

[51] The DHS Mixed Systems Policy, initially issued on January 19, 2007, was revised slightly on January 7, 2009. It is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf. The Mixed Systems Policy is discussed in more detail in the DHS Privacy Office's 2009 Annual Report, which is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf.

b. DHS TRIP

Now in its fourth year of operations, DHS TRIP continued to offer one-stop redress services to the public by providing a centralized processing point for individual travelers to submit redress inquiries.[52] The Chief Privacy Officer is a member of the DHS TRIP Advisory Board. To date, DHS TRIP has received and processed more than 135,000 requests for redress and has an average response time (from the time of first submission to final resolution) of approximately 77 days. DHS TRIP continues to leverage the TSA Secure Flight program, which conducts passenger watch list matching against all Terrorist Screening Database entries containing full name and date of birth (which includes the No Fly List and Selectee List) and the Centers for Disease Control and Prevention Do Not Board List for commercial travel.

An individual begins the DHS TRIP process by submitting a redress inquiry online through the DHS.gov website (or mailing directly to DHS TRIP). The individual is encouraged to submit copies of identity documentation such as a valid driver's license or current passport. The individual's information is reviewed by DHS TRIP and provided to the appropriate government agency (agencies) for adjudication, which includes reviewing and, if appropriate, updating information that may be contained in government databases. When the adjudication is complete, DHS TRIP sends the individual a letter with the final determination; the letter also contains information regarding the reviewability of the decision.

c. US-VISIT Redress Program

One of the main goals of the US-VISIT redress program is to maintain and protect the integrity and privacy of the information of the individuals in its systems. The information has to be accurate, timely, relevant, and complete. US-VISIT responded to 1,250 redress requests during the reporting period. In 2010, US-VISIT established a new goal to provide a timely response to 99 percent or more of all redress requests within 20 business days. In FY 2011, 100 percent of the cases were closed within 20 business days, and 71 percent of the cases in 2011 were closed in five days or fewer.

Erroneous personal information may be corrected through the redress process, which, in turn prevents future inconvenience or hardship for legitimate travelers entering the United States or other individuals whose benefits applications depend on Automated Biometric Identification System (IDENT) searches. US-VISIT's redress process allows individuals the opportunity to receive a fair, timely, and independent review of issues or concerns regarding the collection and use of their biometric and biographic information. Redress requests may be submitted through the DHS TRIP program and additionally by emails, fax or mail directly to US-VISIT. If an individual is not satisfied with the correction from US-VISIT, he or she may appeal redress decisions to the Department's Chief Privacy Officer. Additional information on US-VISIT's privacy-related activities is included in Part One, Section VIII.E and Appendix II.G.

[52] The DHS Privacy Office's 2010 Annual Report (page 74) contains more information. This Report is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2010.pdf.

d. Transportation Sector Threat Assessment and Credentialing Redress

TSA's Office of Transportation Threat Assessment and Credentialing (TTAC) 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. TTAC provides daily checks on over 12 million transportation sector workers against federal watch lists. TTAC 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. Over the past year, TTAC granted 12,757 appeals and denied 1,143. Additionally, TTAC granted 3,448 waivers and denied 211.

III. Reporting

Public reporting is an essential component of the DHS Privacy Office's efforts to further transparency of the Department's privacy-related activities. The Office issues congressionally-mandated public reports that document progress in implementing DHS privacy policy and FOIA policy. All of these reports are available on the DHS Privacy Office website. Office staff members also provide briefings to the Congress on privacy and FOIA-related matters upon request. These activities demonstrate the Department's commitment to transparency and public accountability. During the reporting period, the DHS Privacy Office:

- issued three quarterly reports to Congress required by Section 803 of the 9/11 Commission Act. These reports include: (1) the number and types of 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 complaints received by the Department for alleged violations, and (4) a summary of the disposition of such complaints and the reviews and inquiries conducted. They also include information on PTAs; PIAs; SORNs and associated Privacy Act Exemptions; Privacy Act (e)(3) Statements; Computer Matching Agreements;[53] and privacy protection reviews of IT and program budget requests, including OMB 300s and Enterprise Architecture Alignment requests through the DHS Enterprise Architecture Board;[54]
- submitted the 2010 Annual FOIA Report to the Attorney General of the United States. This report provides summary and 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;
- published the second annual Chief FOIA Officer Report in March 2011 as required by the Attorney General's March 19, 2009 memorandum, *Freedom of Information Act Memorandum for the Heads of Executive Departments and Agencies*.[55] This report discusses actions taken by the DHS Privacy Office to apply the presumption of openness, ensure that DHS has an effective system for responding to requests, increase proactive disclosure, fully utilize technology, reduce backlogs, and improve response times; and
- issued the 2010 DHS Data Mining Report to Congress, as required annually by The Federal Agency Data Mining Reporting Act of 2007.[56] The report describes DHS activities already deployed or under development that fall within the Act's definition of data mining. The Report describes in detail four DHS programs: the Automated

[53] As required under the Privacy Act 5 U.SC. § 552a(8).
[54] DHS Section 803 Reports dating back to December 2007 are available on the DHS Privacy Office website, http://www.dhs.gov/files/publications/editorial_0514.shtm#2.
[55] www.justice.gov/ag/foia-memo-march2009.pdf.
[56] 42 U.S.C. § 2000ee-3.

Targeting System (ATS) Inbound and Outbound (Cargo) and ATS Passenger modules administered by CBP; the Data Analysis and Research for Trade Transparency System administered by ICE; and the Freight Assessment System administered by TSA.[57]

- None of these programs make decisions about individuals solely on the basis of data mining results. The DHS Privacy Office continues to monitor each of these programs to ensure that privacy protections are implemented. Should any other Department programs seek to engage in data mining in the future, the DHS Privacy Office will work with them to build in privacy by design and will describe their activities in future data mining reports.

During this reporting period, the DHS Chief Privacy Officer testified at one congressional hearing, and she and DHS Privacy Office staff conducted numerous other briefings.

- On July 22, 2010, the Chief Privacy Officer briefed Senate Homeland Security and Government Affairs Committee (HSGAC) staff on FOIA.
- On August 17, 2010, the Chief Privacy Officer participated with representatives of NPPD, DoD, and the NSA in two joint briefings on cybersecurity issues for members of the HSGAC and the House Committee on Homeland Security.
- On August 30, 2010, the Chief Privacy Officer, Deputy Chief Privacy Officer and other Privacy Office staff briefed the HSGAC minority staff on the work of the DHS Privacy Office and provided an update on judicial redress under the Privacy Act.
- On September 14, 2010, the Chief Privacy Officer and Deputy Chief Privacy Officer briefed Senator John Kerry's staff and Senate Commerce Committee staff on the December 2008 DHS Privacy Policy Memorandum 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*.[58]
- On September 17, 2010, the Chief Privacy Officer briefed the House Committees on Homeland Security and Oversight and Government Reform minority staff on FOIA backlog reduction efforts and FOIA processing procedures.
- On December 1, 2010, the Chief Privacy Officer briefed the Senate HSGAC staff on the DHS Privacy Office Annual Report.
- On December 14, 2010, the Chief Privacy Officer and other Privacy Office staff held a conference call with the Senate HSGAC staff to discuss proposed revisions to the Privacy Act.
- On February 10, 2011, the Chief Privacy Officer provided an additional briefing to HSGAC Committee minority staff on DHS FOIA processing.
- On March 2-4 and March 14, 2011, Privacy Office FOIA staff participated in transcribed depositions to the House Committee on Oversight and Government Reform regarding the DHS FOIA program.

[57] http://www.dhs.gov/xlibrary/assets/privacy/2010-dhs-data-mining-report.pdf.
[58] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

- On March 3, 2011, the Deputy Chief Privacy Officer presented an overview of Privacy Office functions at a budget briefing for the Senate Homeland Security Appropriations Sub-Committee staff.
- On March 31, 2011, the Chief Privacy Officer appeared as a sworn witness before the House Oversight and Government Reform Committee hearing on DHS FOIA processes.

IV. DPIAC

The DHS Data Privacy and Integrity Advisory Committee (DPIAC) is chartered under the Federal Advisory Committee Act[59] to provide advice to the Secretary of Homeland Security and the Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to PII, data integrity, and other privacy-related matters. 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.

During this reporting period:

- The DPIAC held quarterly public meetings in September 2010, March 2011, and May 2011. At each meeting, the Chief Privacy Officer updated the Committee on the DHS Privacy Office's activities. The Privacy Officers for CBP, USCIS, and S&T briefed the Committee on their components' implementation of DHS privacy policy during the September, March, and May meetings, respectively; and
    - Other meeting highlights include a presentation by Howard Schmidt, Cybersecurity Coordinator and Special Assistant to the President, on the Obama Administration's cybersecurity initiatives, and briefings by DHS Privacy Office staff on the Office's new compliance review process, on DHS privacy training programs, and on privacy protections for the Department's use of social media.
- At the Chief Privacy Officer's request, the DPIAC undertook a review of the Department's internal infrastructure for information sharing among DHS components. This on-going review will lead to recommendations on the potential privacy impacts of information sharing infrastructure in a report to be issued later this year.

All DPIAC reports, meeting agendas, meeting minutes, and, when available, transcripts are posted on the DHS Privacy Office website. New DPIAC members joined the Committee on July 11, 2011; their contributions will be discussed in the next Annual Report.

[59] 5 U.S.C. App. 2.

Part Three – Making a Difference: Advancing International Privacy

The DHS Privacy Office is an integral member of the Department's international team. Led by the Directors of International Privacy Policy (IPP), the Office's contributions have made a difference in support of DHS and the federal government on numerous high-profile international information sharing initiatives. Part Three of this Report summarizes key activities and accomplishments in the international arena.

I. Impact on International Engagement

The DHS Privacy Office regularly advises DHS components and federal partners on international information sharing agreements, negotiations, and other engagements to ensure consistency with DHS privacy policy, the ISE Privacy Guidelines, and fulfillment of compliance requirements, where relevant. During this reporting period, the Office participated in the several international engagements.

- U.S. – EU Passenger Name Record (PNR) Agreement - The Department, led by the DHS Deputy Secretary, engaged in renegotiation of the 2007 U.S. – EU PNR Agreement during the reporting period. The Chief Privacy Officer served as one of the core members of the Deputy Secretary's negotiating team. The DHS Privacy Office contributed background and analysis of EU data protection policies and concerns, and provided outreach to EU and Member State officials. Section II.H of Appendix II includes additional information on the Office's PNR related activities.
- U.S. – Canada Shared Vision for Perimeter Security and Economic Competitiveness[60] - In February 2011, President Obama and Canadian Prime Minister Harper announced a broad initiative for enhanced cooperation to increase security and accelerate the legitimate flow of people, goods, and services across the U.S.-Canada border. One of the cornerstones of the initiative is development of U.S.- Canada privacy protection principles to inform and guide the *Vision* initiatives. The Chief Privacy Officer and the DOJ Chief Privacy and Civil Liberties Officer are the U.S. co-leads for these principles for information sharing.
- U.S. – EU Data Protection and Privacy Agreement (DPPA) - In March 2011, the U.S., co-led by DHS, the Department of State, and DOJ, began formal negotiations with the European Commission on the DPPA. The DPPA is intended to establish mutual recognition through the acknowledgement of baseline standards for protecting information exchanged for law enforcement, criminal justice, and public security

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

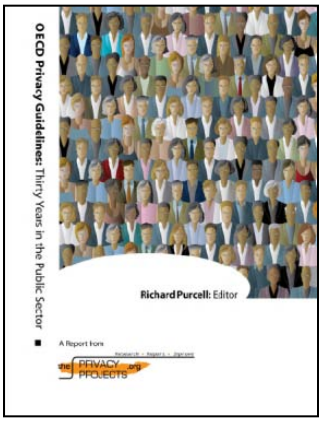
purposes. The DHS Privacy Office is a member of the DHS negotiating team, providing subject matter expertise for this ongoing effort.

- Preventing and Combating Serious Crimes (PCSC) Agreements - PCSC Agreements, which allow for the exchange of biometric and biographic data and are required of all Visa Waiver Program (VWP) countries under the 9/11 Commission Act, are a significant advancement in cross-border information sharing. The DHS Privacy Office provided subject matter expertise for the U.S. negotiating team, informed VWP partners of privacy protections imbedded into the PCSC program, and encouraged them to adopt DHS privacy best practices.
- The Five Country Conference (FCC) - The FCC is a forum for cooperation on migration and border security between the countries of Australia, Canada, New Zealand, the United Kingdom, and the United States. The DHS Privacy Office worked with Department leads to ensure that resulting information sharing agreements are consistent with DHS privacy policy and the ISE Privacy Guidelines, and that compliance requirements are satisfied.

II. Educational Outreach and Leadership

The DHS Privacy Office leads in educational outreach to the federal and international communities, increasing understanding of the U.S. privacy framework and presenting DHS privacy policies and practices as a model. During the reporting period, the Office:

- continued to develop international privacy policy training for DHS employees deployed to international posts. This training will raise officers' awareness before deployment and increase their knowledge on how to respond to issues regarding U.S. privacy law or DHS Privacy Policy that may arise at post. This training is also discussed in Part One, Section VII;
- continued to encourage international partners to adopt privacy best practices, such as implementation of internationally recognized FIPPs and to use model compliance documents, such as the DHS PIA;[61]



- sponsored a study (shown at right) by The Privacy Projects, a non-profit organization of recognized privacy professionals, on how the Organization for Economic Cooperation and Development (OECD) Privacy Guidelines have influenced the development of laws, regulations and public policy in five representative OECD member states -- Australia, Canada, Japan, Spain, and the United States;[62] and

[61] The DHS Privacy Impact Assessment template and guidance, and other guidance documents prepared by the DHS Privacy office, are available on the Office's website at http://www.dhs.gov/files/publications/gc_1209396374339.shtm.
[62] The study is available at http://theprivacyprojects.org/wp-content/uploads/2009/08/FINAL-OECD-PRIVACY-GUIDELINES-PUBLIC-SECTOR.pdf.

- continued to support engagement with foreign government counterparts through participation in the State Department's international visitor exchange programs. The IPP Group contributed to five programs with participants from ten countries.

III. Interpreting International Data Protection Frameworks

The DHS Privacy Office actively monitors trends in global privacy to guide DHS objectives and to stay abreast of international developments. Multilateral and bilateral engagements improve the Office's analysis capabilities and provide a forum for in-depth discussion and debate. During the reporting period, the Office:

- contributed to the interagency privacy work of the OECD Working Party for Information Security and Privacy. A major undertaking this year was the review of the 1980 OECD Privacy Guidelines, a foundation for privacy law and policy in many countries and organizations throughout the world. DHS Privacy Office staff often participated as the sole representative of the public sector perspective, especially concerning law enforcement and security;
- participated in interagency discussions regarding efforts within the Organization of American States to develop guiding privacy principles; and
- continued to observe the work of the Council of Europe's Consultative Committee of Experts to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which serves as the backbone of international privacy law in over 40 European countries. The IPP Group coordinated United States Government comments on the Council's Consultation on the Modernization of Convention 108.[63] The United States Government comments recommend that any revision of the Convention include specific provisions that authorize access to personal data and sharing of personal data between states for legitimate law enforcement and public security purposes.

More information on the DHS Privacy Office's international activities is included in Appendix II. H.

[63] The United States Government comments are available starting on page 369 at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/T-PD-BUR_2011_01_%20prov_MOS_12_05_11_PUBLIC.pdf.

The Future of Privacy at DHS

The DHS Privacy Office, and the entire DHS Privacy infrastructure including component privacy officers, PPOCs, and program managers, make a difference everyday as we strive to embed privacy protections in everything the Department does while also supporting the Department's mission. This approach to privacy is an example of effective privacy protections, making certain we are involved in all aspects of DHS programs' life cycles, and integrated into the Department's responsibilities, which include protecting privacy.

As the value of personal information continues to grow in importance, together with the need to share it, privacy impacts will also grow proportionately. This will continue to create a demand for privacy professionals on the ground and at a strategic level, making the DHS Privacy Office and the component officers even more essential to the future mission of DHS.

During the next reporting period, the DHS Privacy Office expects that many of the focuses from this year --cybersecurity, domestic and international information sharing, cloud computing, fusion centers -- will demand even greater attention.

Improved implementation of the FIPPs will strengthen the Department's compliance and accountability framework, and the Office's enhanced compliance mechanisms will ensure PII is used properly. Further, the Office will strengthen its incident-handling procedures for mitigating privacy incidents and preventing their recurrence. The FIPPS will remain central to our efforts to building a stronger privacy program at DHS.

APPENDICES

Appendix I – Background and Reference

A. Acronym List

Acronym List	
AIT	Advanced Imaging Technology
ATR	Automated Target Recognition
ATS	Automated Targeting System
CBP	U.S. Customs and Boarder Protection
CCTV	Closed Circuit Television
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Office of the Chief Information Security Officer
CMA	Computer Matching Agreement
CRCL	Civil Rights and Civil Liberties
CTAC	Commercial Targeting and Analysis Center
CWIN	Critical Infrastructure Warning Information Network
DIB	Data Integrity Board
DOJ	Department of Justice
DPIAC	Data Privacy and Integrity Advisory Committee
DPPA	Data Protection and Privacy Agreement
EAB	Enterprise Architecture Board
EOC	Enterprise Operations Center
ESC	Executive Steering Committee
EU	European Union
FCC	Five Country Conference
FEMA	Federal Emergency Management Agency
FICAM / ICAM	Federal Identity, Credential, and Access Management
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
FY	Fiscal Year
GAO	Government Accountability Office
GPO	Government Printing Office
HIR	Homeland Intelligence Reports
I&A	Office of Intelligence and Analysis
IAPP	International Association of Privacy Professionals
ICE	U.S. Immigration and Customs Enforcement
IdM	Identity Management
IdP	Identity Proofing
IPC	Interagency Policy Council
IPP	International Privacy Policy
ISE	Information Sharing Environment
ISGB	Information Sharing Governance Board
IT	Information Technology
LPR	Legal Permanent Resident
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCTC	National Counterterrorism Center
NICC	National Infrastructure Coordinating Center

Acronym List	
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
NSA	National Security Agency
NSS	National Security Staff
NSTIC	National Strategy for Trusted Identities in Cyberspace
OCIO	Office of the Chief Information Officer
OECD	Organization for Economic Cooperation and Development
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPS	Operations Coordination and Planning
OTC	Office of Transformation Coordination
PCR	Privacy Compliance Review
PCSC	Preventing and Combating Serious Crime
PIA	Privacy Impact Assessment
PIHG	Privacy Incident Handling Guidance
PII	Personally Identifiable Information
PNR	Passenger Name Record
POTS	Privacy Office Tracking System
PPOC	Privacy Point of Contact
PRA	Paperwork Reduction Act
Privacy Act	Privacy Act of 1974
PRB	Program Review Board
PTA	Privacy Threshold Analysis
RBPS	Risk Based Performance Standards
S&T	Science and Technology Directorate
SAR	Suspicious Activities Reporting
SORN	System of Record Notice
SSN	Social Security Number
TRIP	Traveler Redress Inquiry Program
TSA	Transportation Security Administration
TTAC	Office of Transportation Threat Assessment and Credentialing
UIDAI	Unique Identification Authority of India
U.K.	United Kingdom
US-CERT	U.S. Computer Emergency Readiness Team
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	U.S. Secret Service
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology Program
VWP	Visa Waiver Program

B. DHS Implementation of the FIPPs

DHS's implementation of the FIPPs[64] is described below.

[64] *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.

- **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 (NARA).
- **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.

C. Published PIAs

The table below lists all PIAs published between July 1, 2010 and June 30, 2011.

Component	Name of System	Date Approved
TSA	**DHS/TSA/PIA-028,** MyTSA Mobile Application	7/1/2010
TSA	**DHS/TSA/PIA-029,** Operations Center Incident Management System Update	7/12/2010
USSS	**DHS/USSS/PIA-002,** Targeted Violence Information Sharing System	7/13/2010
DHS-wide	**DHS/ALL/PIA-027,** Watchlist Service	7/14/2010
DHS-wide	**DHS/ALL/PIA-026(a),** iComplaints	715/2010
ICE	**DHS/ICE/PIA-015(b),** Enforcement Integrated Database Update	8/4/2010
S&T	**DHS/S&T/PIA-019,** Iris and Face Technology Demonstration and Evaluation	8/13/2010

Component	Name of System	Date Approved
ICE	**DHS/ICE/PIA-023,** Significant Event Notification System	8/13/2010
DHS-wide	**DHS/ALL/PIA-028,** Freedom of Information Act and Privacy Act Records Program	8/23/2010
DHS-wide	**DHS/ALL/PIA-029,** Entellitrak	8/30/2010
DHS-wide	**DHS/ALL/PIA-027(a),** Watchlist Service Update	9/7/2010
USCIS	**DHS/USCIS/PIA-031,** Citizenship and Immigration Data Repository	9/8/2010
TSA	**DHS/TSA/PIA-030,** Access to Sensitive Security Information in Contract Solicitations	9/14/2010
DHS-wide	**DHS/ALL/PIA-031,** Wide Social Networking Interaction and Applications	9/16/2010
DHS-wide	**DHS/ALL/PIA-030,** Eversity	9/24/2010
ICE	**DHS/ICE/PIA-020(a),** Alien Criminal Response Information Management System & Enforcement Integrated Database Update	9/29/2010
USCIS	**DHS/USCIS/PIA-032,** National File Tracking System	10/11/2010
S&T	**DHS/S&T/PIA-008(a),** Standoff Technology and Integration and Demonstration Program Update	10/14/2010
ICE	**DHS/ICE/PIA-024,** Electronic Surveillance System	11/2/2010
USCIS	**DHS/USCIS/PIA-033,** Immigration Benefits Background Check Systems	11/5/2010
FEMA	**DHS/FEMA/PIA-015,** Quality Assurance Recording System	11/10/2010
USSS	**DHS/USSS/PIA-003,** Protective Research Information System Management Update	11/12/2010
DHS-wide	**DHS/ALL/PIA-032,** DHS Information Sharing Environment Suspicious Activity Reporting Program	11/17/2010
S&T	**DHS/S&T/PIA-020,** Science & Technology Enterprise Volunteers	12/2/2010
ICE	**DHS/ICE/PIA-025,** Electronic Discovery Software System	12/10/2010
OPS	**DHS/OPS/PIA-008,** Patriot Report Database	12/10/2010
TSA	**DHS/TSA/PIA-031,** Exit Lane Breach Control System	12/28/2010
CBP	**DHS/CBP/PIA-009,** TECS Primary and Secondary	12/23/2010
NPPD	**DHS/NPPD/PIA-017,** National Infrastructure Coordinating Center Suspicious Activity Reporting Initiative	12/29/2010
OPS	**DHS/OPS/PIA-007,** OPS Publicly Available Social Media Monitoring and Situational Awareness Initiative Update	1/6/2011
ICE	**DHS/ICE/PIA-005(b),** Bond Management Information System Web Release 2.2	1/19/2011
USCIS	**DHS/USCIS/PIA-034,** H-1B Visa Cap Registration	1/28/2011
TSA	**DHS/TSA/PIA-032,** TSA Advanced Imaging Technology Update	2/1/2011
OPS	**DHS/OPS/PIA-009,** National Operations Center Tracker and Senior Watch Officer Logs	2/3/2011
USCIS	**DHS/USCIS/PIA-035,** Migrant Information Tracking System	2/3/2011
DHS-wide	**DHS/ALL/PIA-034,** Medical Credentials Management System	2/11/2011
USCIS	**DHS/USCIS/PIA-036,** E-Verify Self-Check	3/4/2011
S&T	**DHS/S&T/PIA-021,** Cell All	3/7/2011
USCG	**DHS/USCG/PIA-015,** Merchant Mariner Licensing and Documentation System	3/7/2011
ICE	**DHS/ICE/PIA-026,** Federal Financial Management System	3/24/2011
DHS Wide	**DHS/ALL/PIA-038,** Integrated Security Management System	3/24/2011
DHS Wide	**DHS/ALL/PIA-037,** SharePoint and Collaboration Sites	3/24/2011
Management	**DHS/MGMT/PIA-005,** Foreign National Visitor Management System	3/31/2011
ICE	**DHS/ICE/PIA-027,** ICE Subpoena System	4/1/2011

Component	Name of System	Date Approved
FEMA	**DHS/FEMA/PIA-016,** Application and Registration Records for Training and Exercise Programs	4/7/2011
USCG	**DHS/USCG/PIA-016,** College Board's Recruitment Plus	4/11/2011
NPPD	**DHS/NPPD/PIA-002,** Critical Infrastructure Warning Information Network 3-Year Review	4/19/2011
NPPD	**DHS/NPPD/PIA-018,** Chemical Facilities Anti-Terrorism Standards Personnel Surety	5/4/2011
S&T	**DHS/S&T/PIA-022,** Biodefense Knowledge Management System	5/4/2011
USCIS	**DHS/USCIS/PIA-030(b),** E-Verify Ride Update	5/6/2011
TSA	**DHS/TSA/PIA-033,** Enterprise Search Portal	5/10/2011
TSA	**DHS/TSA/PIA-034,** Transportation Security Administration Enterprise Performance Management Platform	5/17/2011
TSA	**DHS/TSA/PIA-001(a),** Transportation Threat Assessment Vetting and Credentialing Screening Gateway 3-Year Review	5/18/2011
USCG	**DHS/USCG/PIA-004,** Law Enforcement Information Database/Pathfinder	5/19/2011
ICE	**DHS/ICE/PIA-015(a),** Enforcement Integrated Database Update	5/24/2011
USCIS	**DHS/USCIS/PIA-029(a),** Eligibility Risk and Fraud Assessment Testing Environment Update	6/1/2011
USCIS	**DHS/USCIS/PIA-037,** Standard Lightweight Operational Programming Environment – Rules-Based Tools Prototype	6/2/2011
ICE	**DHS/ICE/PIA-028,** Automated Threat Prioritization	6/6/2011
USCIS	**DHS/USCIS/PIA-010(e),** Person Centric Query Service Supporting Immigration Status Verifiers of the USCIS Enterprise Service Directorate/Verification Division Update	6/8/2011
DHS-wide	**DHS/ALL/PIA-039,** Google Analytics	6/9/2011
USCIS	**DHS/USCIS/PIA-038,** Freedom of Information Act/Privacy Act Information Processing System	6/14/2011
FEMA	**DHS/FEMA/PIA-017,** Federal Emergency Response Repository	6/21/2011
CBP	**DHS/CBP/PIA-001(e),** Advanced Passenger Information System Update National Counter Terrorism Center	6/23/2011
ICE	**DHS/ICE/PIA-001(a),** Student and Exchange Visitor Information System Update National Counter Terrorism Center	6/23/2011
CISOMB	**DHS/CISOMB/PIA-001,** Virtual Ombudsman 3-Year Review	6/29/2011
USCIS	**DHS/USCIS/PIA-027(a),** Refugees, Asylum, and Parole System and the Asylum Pre-Screening System Update National Counter Terrorism Center	6/30/2011

D. Published SORNs

The table below lists all SORNs published in the Federal Register between July 1, 2010 and June 30, 2011.

Component	Name of System	Date Published in the Federal Register
DHS-wide	**DHS/ALL-029,** Civil Rights and Civil Liberties Matters with Privacy Act Exemptions	7/8/2010
USCIS	**DHS/USCIS-012,** Citizenship and Immigration Data Repository with Privacy Act Exemptions	9/8/2010
DHS-wide	**DHS/ALL-031,** DHS Information Sharing Environment Suspicious Activity	9/10/2010

Component	Name of System	Date Published in the Federal Register
	Reporting Program with Privacy Act Exemptions	
NPPD	**DHS/NPPD-001,** National Infrastructure Coordinating Center Records System of Records with Privacy Act Exemptions	11/15/2010
OPS	**DHS/OPS-003,** Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion Records with Privacy Act Exemptions	11/15/2010
OPS	**DHS/OPS-004,** Publicly Available Social Media Monitoring and Situational Awareness Initiative System of Records	2/1/2011
FEMA	**DHS/FEMA-002,** Quality Assurance Recording System	2/15/2011
ICE	**DHS/ICE-004,** Bond Management Information System	2/15/2011
USCIS	**DHS/USCIS-013,** E-Verify Self Check	2/16/2011
OPS	**DHS/OPS-002**, National Operations Center Senior Watch Officer/Tracking Log with Privacy Act Exemptions	3/8/2011
FEMA	**DHS/FEMA-011,** General Training and Exercise Programs with Privacy Act Exemptions	4/6/2011
OHA	**DHS/OHA-001,** Contractor Occupational Health and Immunization Records with Privacy Act Exemptions	4/18/2011
S&T	**DHS/S&T-.0001,** SAFETY Act Records Consolidation	4/18/2011
USCG	**DHS/USCG-002,** Employee Assistance Program	5/3/2011
USCG	**DHS/USCG-007,** Special Needs Program	5/3/2011
TSA	**DHS/TSA-023,** Workplace Violence Prevention Program with Privacy Act Exemptions	5/5/2011
USCG	**DHS/USCG-008,** Court Martial Case Files with Privacy Act Exemptions	5/13/2011
USCG	**DHS/USCG-024,** Auxiliary Database	5/18/2011
USCIS	**DHS/USCIS-001,** Alien File, Index and National File Tracking System of Records with Privacy Act Exemptions	6/13/2011
NPPD	**DHS/NPPD-002,** Chemical Facility Anti-Terrorism Standards Personnel Surety Program	6/14/2011

Appendix II – DHS Privacy Office Operations

A. Compliance Activities

1. Privacy Compliance Documents: Keys to Transparency and Accountability

DHS has three main documents related to privacy compliance: (1) the PTA, (2) the PIA, and (3) the SORN. While each of these documents has a distinct function in implementing privacy policy at DHS, together these documents further the transparency of Department activities and demonstrate accountability.

a. PTAs

The PTA is the first document completed by DHS staff seeking to implement or modify a system, program, technology, or rulemaking. The PTA is reviewed and adjudicated by the Compliance Group and serves as the official determination as to whether the system, initiative, or program is privacy sensitive (i.e., used to collect and maintain PII) and requires additional privacy compliance documentation such as a PIA or SORN.

During the reporting period, the DHS Privacy Office reviewed and validated 585 PTAs.

b. PIAs

The E-Government Act and the Homeland Security Act require PIAs, and PIAs may be required in accordance with the Chief Privacy Officer's statutory authority. PIAs are an important tool for examining the privacy impact of IT systems, initiatives, programs, technologies, or rule-makings. The PIA is based on the FIPPs framework and touches on general areas such as scope of information collected, 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 preceding section's 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 early stages.

If a PIA is required, the program 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 Group for review and approval. The Chief Privacy Officer conducts a final review before signing. Once approved, the PIA is made publicly available on the DHS 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.

During the reporting period, the DHS Privacy Office reviewed and validated 68 PIAs.

c. 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 Compliance Group. As with the PIA, the Chief Privacy Officer reviews, signs, and publishes all SORNs for the Department. Once the PTA, PIA, and SORN are completed, the documents must be periodically reviewed by the Compliance Group (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.[65]

During the reporting period, the DHS Privacy Office reviewed and validated 20 SORNs and associated Privacy Act exemptions.

2. 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 (DIB) to oversee and approve their use of computer matching programs.[66] The DHS DIB is responsible for approving and overseeing the use of computer matching programs by the Department. The Chief Privacy Officer serves as the Chairman and DIB members include the Inspector General and

[65] Office of Mgmt. & 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.

[66] 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).

representatives of components that currently have active Computer Matching Agreements (CMA) in place.[67]

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 DIB. CMAs must be entered into 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.[68]

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.

During the reporting period, DHS recertified the following existing Computer Matching Agreements for the period of 12 months allowable by statute:

- one 12-month CMA recertification, extending a computer matching program between USCIS and the State of New Jersey Department of Labor and Workforce Development;
- one 12-month CMA recertification, extending a computer matching program between USCIS and the State of New York Department of Labor;
- one 12-month CMA recertification, extending a computer matching program between USCIS and the State of Massachusetts Division of Unemployment Assistance;
- one 12-month CMA recertification, extending a computer matching program between USCIS and the State of California Department of Health Care Services; and
- one 12-month CMA recertification, extending a computer matching program between USCIS and the State of Texas Workforce Commission.

3. Additional Compliance Reporting and Oversight

In collaboration with the CIO, CISO, and Chief Financial Officer (CFO), the Compliance Group identifies programs that must go through the privacy compliance process through several avenues including: (1) the FISMA Certification and Accreditation (C&A) process; (2) the OMB IT budget submission process; (3) CIO IT Program Reviews; and (4) Paperwork Reduction Act (PRA) processes. Through these collaborations, the Compliance Group provides subject matter expertise for reviews of new IT programs and newly budgeted programs to identify privacy compliance issues.

4. FISMA Privacy Reporting

Privacy and information security are closely linked, and strong practices in one area typically support the other. Ensuring security of PII is one of the FIPPs. To that end, the Compliance Group works closely with the CISO to monitor privacy requirements under FISMA. On a

[67] 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).
[68] 5 USC § 552a(o).

quarterly and annual basis, DHS reports to OMB its progress in conducting PIAs and issuing SORNs for IT systems that are required to go through the FISMA C&A process. At the end of the reporting period, DHS's FISMA privacy numbers were 77% for PIAs and 95% for SORNs. The DHS Privacy Office established a goal of 80% for PIAs by the end of the fiscal year.

5. OMB IT Budget Submissions

All major DHS IT programs are reviewed by the Compliance Group on an annual basis, prior to submission to OMB for inclusion in the President's annual budget.[69] The Department continues to require that IT program budget submissions demonstrate, among other things, that the agency has properly addressed privacy. The Compliance Group plays a substantial role in the review of the OMB budget submissions (known as Exhibit 300s) prior to submission to OMB. Also referred to as the OMB 300 process, the Compliance Group's review is both substantive and procedural, ensuring that each investment has the proper privacy documentation in place at the correct time. Specifically, the review of each investment portfolio includes an examination of the privacy protections implemented within the individual systems associated with that investment, and whether the protections are documented in a PIA or SORN. The Compliance Group evaluates and scores each investment based on its responses to a standardized set of questions and ensures that the appropriate documentation has been completed. The Compliance Group then works with each investment program manager to complete necessary documents. The Compliance Group works in close cooperation with the DHS CIO and CFO to ensure that the Department's IT investments meet the established legal and policy standards set forth by DHS, OMB, and Congress.

During the FY 2012 budget review process, the Compliance Group reviewed DHS investments and associated systems. To receive a passing score, submissions had to include the appropriate privacy documentation or have a completed PTA on file if the Compliance Group determined the investment would not require additional privacy documentation. Based on these requirements, the Compliance Group failed nine IT investments through the OMB 300 scoring process due to insufficient privacy protections and privacy documentation.[70] However, the Compliance Group supported an additional six IT investments with resolving privacy issues by completing PIAs and SORNs.

At the end of the reporting period, the Compliance Group was in the process of scoring FY 2013 investments in preparation of planning activities to occur at the outset of FY 2012. The review process occurs two years in advance.

6. Paperwork Reduction Act (PRA) and Forms

The Compliance Group also broadened its reach this reporting period through engaging in the PRA and associated forms process at the Department. Privacy Act e(3) statements are required by the Privacy Act to appear on government forms that collect PII and are part of formal notice providing transparency to the person about whom the information is being collected. The requirements of Privacy Act e(3) statements and PRA forms that are used as part of information

[69] *See* Office of Mgmt. & 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/circulars/a11/current_year/s300.pdf.

[70] An IT investment failing the OMB scoring process provides DHS management, including component privacy officers and PPOCs, as well as the CIO, with necessary visibility into privacy compliance documentation gaps thereby elevating management's attention to closing these gaps.

collection requests are closely intertwined. For that reason, the Compliance Group has developed a close working relationship with the PRA Program Management Office within OCIO. As a result, the Compliance Group is well-positioned to review forms and ensure that information collected on a form is only the information needed to fulfill the purpose of the collection. Additionally, these reviews provide an opportunity for the Compliance Group to review Privacy Act e(3) statements that are provided to individuals at the time of collection. The Compliance Group provided training at PRA workshops, attended monthly and quarterly PRA point of contact meetings, and coordinates regularly with the PRA Program Management Office within OCIO.

7. Program Review Board

The Chief Privacy Officer is fully engaged in the work of the DHS Deputy Secretary's Program Review Board (PRB), a senior leadership group that looks for operational, intelligence, and strategic synergies across the Department to eliminate redundancies and protect the Department's resources. The goals of the PRB are to improve the linkage of strategy to programs and budgets, to increase stability of the Future Years Homeland Security Program,[71] and to maintain fiscal discipline. The PRB provides the DHS Privacy Office another window into Department programs and initiatives that may have implications for privacy.

B. Privacy Incidents and Inquiries

1. DHS Privacy Incident Response Plan

During this reporting period, the DHS Privacy Office revisited the *DHS Privacy Incident Handling Guidance* (PIHG), the primary resource for privacy incident policy within DHS, in collaboration with DHS component privacy incident stakeholders. The Office anticipates the final updated version will be available by the end of the calendar year.[72] The PIHG informs DHS components, employees, and contractors of their obligation to protect the PII they are authorized to handle and explains how to respond to suspected or confirmed privacy incidents. The PIHG adheres to OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (OMB M-07-16),[73] which is the foundation for the management and reporting of all privacy incidents across the federal government.

Privacy incidents can occur within both the unclassified and classified realms of information at DHS. Strict adherence to DHS Directive 4300A and *DHS 4300A Sensitive Systems Handbook* (DHS 4300A Handbook) as well as the CISO Concept of Operations, enables the DHS Privacy Office, the CIO, and the CISO to monitor and mitigate all types of privacy and security incidents. Through continued close collaboration, the Chief Privacy Officer, the CIO, the CISO, and the EOC ensure that all of the Department's privacy and computer security incidents are identified, reported, and responded to appropriately to mitigate harm to DHS-maintained assets and information. While each privacy incident must be evaluated individually, the PIHG provides DHS components, employees, and contractors with a set of guidelines for assessing a situation and responding to a privacy incident in a timely and consistent manner.

[71] 6 U.S.C. § 454.
[72] The current version of the PIHG is available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.
[73] The Memorandum is available at http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.

2. Incident Definitions

The following table sets out the categories of incidents on which the DHS Privacy Office reports together with their category definitions.

Incident Type	Definition
Alteration/Compromise of Information	Includes any incident that involves the unauthorized altering of information, or any incident that involves the compromise of information.
Classified Computer Security Incident	Includes any security incident that involves a system used to process national security information.
Investigation Unconfirmed/Non-Incident	Unconfirmed Incidents are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. Non-Incident is a category DHS uses for incidents that have been determined not to involve the loss of PII.
Malicious Logic	Includes active code such as viruses, Trojan horses, worms, and scripts used by hackers to gain privileges or information, capture passwords, or to modify audit logs to hide unauthorized activity.
Misuse	Involves a violation of federal laws or regulations, or Departmental policies regarding proper use of computer resources; installation of unauthorized or unlicensed software; and accessing resources or privileges that are greater than those assigned.
Unauthorized Access (Intrusion)	Includes all successful unauthorized accesses and suspicious unsuccessful attempts.
Probes and Reconnaissance Scans	Includes probing or scanning of DHS networks for critical services or security weaknesses; data gathering originating from entities known or suspected to be a threat to national security; or probes and scans that appear to be widespread or threatening. This category does not include probes and reconnaissance scans taking place on internet facing connections.

Source: NIST Special Publication 800-61 (Rev.1), *Computer Security Incident Handling Guide*[74]

3. Privacy Incident Handling Quarterly Meetings

The Director of Privacy Incidents and Inquiries held Privacy Incident Handling quarterly meetings in January and May 2011 to enhance the privacy incident handling program at DHS. These fora provided an opportunity for component privacy officers and PPOCs and the DHS EOC managers to share best practices and provide feedback regarding privacy incident management, mitigation, and prevention. Using feedback from the attendees, the Incidents and Inquiries Group presented an anonymized list of incidents and a root cause analysis. The components have used this information to address issues that may arise in their offices.

4. Privacy Complaints by Quarter

Table 3 provides the categories and disposition of complaints the DHS Privacy Office received per quarter Fourth Quarter FY 2010 through Third Quarter FY 2011. The reporting period for these complaints runs quarterly from June 1, 2010 – May 31, 2011, as required by FISMA. Table 4 provides a summary of the data presented in Table 3.

[74] The guide is available at: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

Type of Complaint	Number of Complaints received during this reporting period	Disposition of Complaint		
		Closed - Responsive Action Taken	In Progress (Current Period)	In-Progress (Prior Periods)
Fourth Quarter FY 2010 (June 1, 2010 – August 31, 2010)				
Process and Procedure	6	6	0	0
Redress	6	6	0	2
Operational	61	55	11	2
Referred	8	8	0	0
Total	***81***	***75***	***11***	***4***
First Quarter FY 2011 (September 1, 2010 - November 30, 2010)				
Process and Procedure	5	5	0	0
Redress	1	0	1	2
Operational	58	59	6	6
Referred	10	5	5	1
Total	***74***	***69***	***12***	***9***
Second Quarter FY 2011 (December 1, 2010 – February 28, 2011)				
Process and Procedure	5	5	0	0
Redress	6	7	0	2
Operational	149	132	21	8
Referred	4	9	0	1
Total	***164***	***153***	***21***	***11***
Third Quarter FY 2011 (March 1, 2011– May 31, 2011)				
Process and Procedure	6	4	2	0
Redress	4	4	0	2
Operational	283	278	27	6
Referred	2	1	1	1
Total	***295***	***287***	***30***	***9***

Table 3: DHS Privacy Complaints Received by Quarter

Type of Complaint	Number of Complaints	Disposition of Complaint	
		Responsive Action Taken	No Action Required
Fourth Quarter FY 2010 to Third Quarter FY 2011 (June 1, 2010 - May 31, 2011)			
Process and Procedure	22	20	2
Redress	17	17	9
Operational	551	524	87
Referred	24	23	9
Total	***614***	***584***	***107***

Table 4: DHS Privacy Complaints: Total Received From Fourth Quarter FY 2010 Through Third Quarter FY 2011[75]

[75] The totals in Table 4 reflect complaints received in the reporting period. The totals also include complaints from the previous fiscal year that have not yet been resolved.

C. Privacy Information Sharing and Intelligence (PISI)

The Privacy Office serves on five subcommittees of the Information Sharing and Access Interagency Policy Committee.

- Privacy and Civil Liberties - The DHS Chief Privacy Officer serves as a co-chair of this subcommittee, which is responsible for overseeing the continuing relevance of the ISE Guidelines, especially guidelines pertaining to non-federal entities such as fusion centers. In her role as co-chair the DHS Chief Privacy Officer reviewed written privacy policies issued by fusion centers across the nation as discussed in Part One, Section IV.B of this Report.
- Fusion Centers – This Subcommittee is designed to help the fusion centers achieve the four critical operational capabilities of (1) receiving information; (2) analyzing this information through a formal risk assessment process; (3) disseminating threat information; and (4) gathering locally generated information. For each capability the DHS Privacy Office worked to implement privacy and civil liberties protections, which are enabling capabilities for each of the four critical operational capabilities.
- Suspicious Activity Reporting – The DHS Privacy Office is represented on this subcommittee, which is chartered with overseeing the National Suspicious Activity Reporting Initiative.
- Watchlisting and Screening – The DHS Privacy Office supports this subcommittee devoted to improving the federal guidance and processes related to watchlisting and people screening.
- Information Integration – This Subcommittee works to address issues related to data aggregation processes across the federal community. The DHS Privacy Office provides privacy expertise and guidance on issues related to data aggregation processes across the federal community.

D. Privacy Training

The Privacy Office develops and oversees three different types of training for the Department:

1. Mandatory Training

Privacy training is required by the Privacy Act[76] and OMB Circular A-130[77] for all DHS employees and contractors. Introductory privacy training is provided to all new headquarters employees within six months of hire during two required classroom training events: new employee orientation and DHS 101, a two-day course that provides an overview of all DHS components' roles and activities. That training is supplemented by the DHS Privacy Office's mandatory *A Culture of Privacy Awareness* course. The course is available through the Department's web-based learning management system and covers the essentials of the Privacy Act and the E-Government Act. DHS employees and contractors are instructed to use PII only

[76] 5 U.S.C. 552a(e)(9).
[77] Office of Mgmt. & 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.

for authorized purposes and to protect it from misuse or loss. The Office shares the training it develops with components to enable them to leverage the materials and integrate privacy training into their own programs. DHS components have implemented the *A Culture of Privacy Awareness* course through their own learning management systems. Component privacy officers have also developed component-specific privacy training this reporting year, as detailed in Part One, Section VIII of this Report.

2. Supplemental Training

The DHS Privacy Office advises new DHS outbound attachés and liaisons stationed abroad on the policy implications that misunderstandings of U.S. privacy laws and DHS privacy policies may have for international cooperative activities. Strengthening attachés' and liaisons' understanding of these issues before deployment helps them to identify privacy concerns that may impact DHS activities, improve the dialogue with international partners, and help dispel misperceptions. This program, which will include remote learning opportunities, will be formalized during the next reporting period. Part Two, Section VII and Part Three, Section B of this Report provides additional information on the outbound attachés and liaisons training initiative.

3. Compliance Training

The DHS Privacy Office's Compliance Group also conducted a two-day training event for federal employees and contractors. Part One, Section I discusses this training in more detail.

E. Section 803 Report Details

1. Activities Reported

The following table provides the number of Section 803 reviews completed by DHS from June 1, 2010, through May 31, 2011, by type of review.

Type of Review	Number of Reviews
Privacy Threshold Analyses	585
Privacy Impact Assessments	68
System of Records Notices and associated Privacy Act Exemptions	20
Privacy Act (e)(3) Statements	21
Computer Matching Agreements	6
Total Reviews Completed June 1, 2010 through May 31, 2011	700

2. Section 803 Advice and Responses

For purposes of Section 803 reporting, "advice" and "response to advice" include the issuance of written policies, procedures, guidance, training, or interpretations of privacy requirements for circumstances or business processes written by the DHS Privacy Office and approved by DHS leadership.

From June 1, 2010, through May 31, 2011:

- 16,645 DHS personnel attended instructor-led privacy training courses; and
- 206,557 DHS personnel and contractors completed the mandatory annual privacy training course: *A Culture of Privacy Awareness.*

Section 803 Reports also include information on complaints received by the DHS Privacy Office and components, as discussed in Part Two, Section II of this report. Part One, Section VII includes further information on DHS Privacy Office training activities.

F. Public Speaking Engagements

During this reporting period, the DHS Privacy Office staff made the following public presentations:

July 2010

- U.S.-European Dialogue and Workshop, Washington, DC
- Social Security Administration Office of Privacy and Disclosure Biennial Conference, Baltimore, MD
- Electronic Privacy Information Center Privacy Coalition Meeting, Washington, DC

August 2010

- London School of Economics Public Policy Group Interview, Privacy Office, Washington, DC

September 2010

- Organization for the Advancement of Structured Information Standards E-Identity Conference, Washington, DC
- IAPP Privacy Conference (multiple presenters), Baltimore, MD

October 2010

- 32nd Annual International Conference of Data Protection and Privacy Commissioners, Jerusalem, Israel
- US-VISIT Privacy Week: Keynote Speaker on "Protecting Personal Privacy: Why We Care, How We're Helping to Protect"

November 2010

- Federal Privacy Summit (multiple presenters), Washington, DC
- Privacy Summit, Washington, DC
- Wilson Center Publication Launch (Toronto, Canada and Washington, DC)

December 2010

- The Constitution Project, Washington, DC
- IAPP Practical Privacy Series (multiple presenters), Washington, DC

January 2011

- Data Protection Conference, Brussels, Belgium

February 2011

- RSA Conference, San Francisco, CA
- Armed Forces Communications and Electronics Association, Washington, DC

March 2011

- American Bar Association 6th Annual Homeland Security Law Institute Conference, Washington, DC
- IAPP Global Privacy Summit (multiple presenters), Washington, DC
- State and major urban area fusion center directors meeting in advance of the 2011 National Fusion Center Conference, Denver, CO
- 2011 National Fusion Center Conference (multiple presenters), Denver, CO

April 2011

- National Defense University, Information Resource Management College Washington, DC
- Strengthening Civil Liberties & Security: EU-U.S. Cooperation and Data Protection, PNR, and SWIFT Conference, Washington, DC
- Committee on Women in the Profession: Women in IP Breakfast Series – Hot Topics In Privacy, New York, NY
- Microsoft Innovation Outreach Partnership (IOP) Conference, New York, NY

May 2011

- Center for Policy on Emerging Technologies C-PET/RISE Conference (multiple presenters), Washington, DC
- Small Business Administration "Privacy Day", Washington, DC

June 2011

- The Emerging Reality of Big Data…Conference, Washington, DC
- 2011 Computers Freedom and Privacy Conference (CFP) Conference – The Future is Now, Washington, DC
- Gartner Security & Risk Management Summit, Washington, DC
- NIST NSTIC Privacy Workshop, Boston, MA
- Annual Privacy Compliance Workshop (multiple presenters), Washington DC
- National Defense University, Information Resource Management College Washington, DC

G. Complaints and Redress

1. Process for Internal Response to Privacy Concerns

Section 803 of the 9/11 Commission Act and OMB Memorandum 08-09, *New FISMA Reporting Requirements for FY 2008*,[78] require, among other things, that the Department report quarterly to Congress on privacy complaints received and their disposition. A cornerstone of the DHS complaint system is OMB's definition of "complaints" as written allegations of harm or violation of privacy compliance requirements.[79] Complaints may be from U.S. citizens and LPRs, as well as visitors and aliens.[80] Part Two, Section III contains additional information on DHS Privacy Office responsibilities under Section 803.

Section 803 complaints are separated into four categories.

- **Process and procedure.** Issues concerning process and procedure, such as consent, notice at the time of collection, or notices provided in the Federal Register, such as rules and SORNs.

  Example: An individual submits a complaint as part of a rulemaking that alleges the program violates privacy.

- **Redress.** Issues concerning appropriate access, correction of PII, and redress therein.

  Example: Misidentifications during a credentialing process or during traveler screening at the border or at airports.[81]

- **Operational.** Issues related to general privacy concerns and concerns not related to transparency or redress.

  Example: An employee's health information was disclosed to a non-supervisor.

  Example: A supervisor disclosed a personnel file to a future employer.

- **Referred.** The component or the DHS Privacy Office determined that the complaint would be more appropriately handled by another federal agency or other entity and referred the complaint to the appropriate organization.

  Example: An individual has a question about his or her driver's license or Social Security Number, which the DHS Privacy Office refers to the proper agency.

DHS components and the DHS Privacy Office report disposition of complaints in one of two categories.

- **Closed-Responsive Action Taken**. The component or the DHS Privacy Office reviewed the complaint and a responsive action was taken. For example, an individual may provide additional information to distinguish himself from another individual. In some

[78] This Memorandum is available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-09.pdf.
[79] *Id*.
[80] The Department accepts complaints pursuant to the Mixed Systems Policy, which is discussed in Part Two, Section II. B. of this Report.
[81] This category excludes FOIA and Privacy Act requests for access, which are reported annually in the Annual FOIA Report.

cases, acknowledgement of the complaint serves as the responsive action taken. This category may include responsive action taken on a complaint received from a prior reporting period; and

- **In-Progress**. The component or the DHS Privacy Office is reviewing the complaint to determine the appropriate action or response. This category identifies in-progress complaints from both the current and prior reporting periods.

2. Examples of Component Complaint Handling

a. CBP

With increased presence of Border Patrol checkpoints to increase security along the northern border, the CBP INFO Center has seen an increase in the number of complaints regarding privacy and CBP's search authority. CBP has taken proactive steps to make information available regarding Border Patrol checkpoints and the CBP inspection process by posting information on its website at http://www.cbp.gov,[82] producing a publicly available brochure discussing the checkpoints, and by a coordinated public outreach effort with the CBP INFO Center and the Office of Border Patrol. The following are examples of complaints received during this reporting period:

- a U.S. citizen from Vermont contacted the CBP INFO Center requesting information on the Border Patrol's search authority and jurisdiction. A verbal explanation was provided and a follow-up email was sent providing the individual with CBP's search authority, an overview of Border Patrol checkpoints, and per his request links to additional information for research purposes. The individual was satisfied with the information provided; and
- an individual called the CBP INFO Center to file a complaint regarding her treatment during secondary screening. She stated that the on-duty officer questioned her loudly about a pending criminal case, in front of other travelers who were waiting to be processed. The individual claimed it was embarrassing, and violated her privacy. The Supervisory CBP Officer contacted the individual by telephone and was able to resolve her complaint. The Port Director sent a follow-up letter advising the individual to request to speak to a Passenger Service Manager in the future if she is dissatisfied with the screening process.

b. ICE

The ICE Privacy Office received a privacy complaint concerning the complainant's supervisor's instruction to refrain from placing personal appointments on government calendars. Specifically, the employee objected to being unable to place personal appointments and reminders on the calendar and mark them private so others could not view them. The ICE Privacy Office coordinated with the Office of Professional Responsibility and the Office of Employee & Labor Relations to determine the appropriate response, and then responded directly to the complainant

[82] See http://www.cbp.gov/xp/cgov/border_security/border_patrol/border_patrol_ohs/overview.xml, http://www.cbp.gov/xp/cgov/border_security/border_patrol/, https://help.cbp.gov/app/answers/detail/a_id/11/kw/inspection, and http://www.cbp.gov/linkhandler/cgov/border_security/border_patrol/border_patrol_ohs/national_bp_strategy.ctt/national_bp_strategy.pdf.

in a letter. The ICE Privacy Office determined the supervisor was within her authority to instruct her employees not to use the Outlook calendar for personal appointments during the work day.

c. US-VISIT

During this reporting period, US-VISIT received a redress request pertaining to a biometrics issue. An individual complained that he had experienced delays during his last few entries into the United States, causing him inconvenience. US-VISIT reviewed his record and determined that the problem was due to incorrectly labeled finger prints at the port of entry during one of his visits. This caused the prints that were taken on subsequent entries to mismatch against the prints on file. US-VISIT was able to correct his record.

d. TSA

1. The TSA Office of Privacy Policy and Compliance responded to a traveler's complaint and inquiry into whether TSA Transportation Security Officers violated his Health Insurance Portability and Accountability Act (HIPAA) rights by screening his Continuous Positive Airway Pressure (CPAP) machine in public. CPAP Machines are used primarily in the treatment of sleep apnea. TSA responded to the individual by acknowledging that TSA recognizes the sensitivities regarding screening procedures for persons with medical conditions at security checkpoints. TSA also advised the traveler that TSA is not a "covered entity" under HIPAA. In addition, TSA provided the individual a link to information from TSA's website for travelers with special needs and identified a specific link for more information on CPAP screening.

2. Following media reports that TSA would implement new pat-down procedures, TSA received complaints from several individuals who were upset by their experience. TSA understands that while passengers may differ in their level of comfort with screening procedures, TSA is committed to ensuring that all of its personnel are fully trained to carry out their responsibilities professionally and according to appropriate standards. TSA works with a variety of groups to determine appropriate methods to address public concerns, and to implement appropriate training.

3. TSA received a complaint from an employee stating that TSA personnel mishandled medical information that was attached to an advance leave request. The employee also expressed concerns that the individuals tasked to input the data did not have a need to know the information in the performance of their official duties. After investigating the situation, the TSA Office of Privacy Policy and Compliance determined that the individuals assigned to process the leave request viewed the medical information as supporting documentation to assist in the approval process. In addition, the TSA Office of Privacy Policy and Compliance discovered that TSA leadership at the employee's facility designated personnel outside of the Human Resources Department to process personnel-related documents in order to provide additional administrative resources. Therefore, the processors maintained a need to know the information. The employee subsequently rescinded the complaint.

H. International Privacy Policy

Significant research and analysis, coordination, diplomacy and outreach play a part in the DHS Privacy Office's international engagement efforts. As part of the U.S. Government interagency team, the Privacy Office remains a stable resource across various regions and issues. Doing so entails preparing briefing materials, contributing to international engagement strategies, researching international privacy frameworks, respecting diplomatic concerns, and understanding U.S. privacy law. The following discussion provides a more specific look into the Office's international activities during this reporting period.

1. International Agreements

U.S. – EU PNR Agreement – The Office supported Departmental engagement efforts throughout negotiations of this Agreement, including:

- hosting Members of the European Parliament at the National Targeting Center (NTC) to demonstrate DHS use of PNR and discuss issues specifically concerning the 2007 U.S.-EU PNR Agreement and DHS' privacy policies and protections. The Members led the European Parliament's review of the Agreement and have significant say in its ultimate passage;
- participating in an NTC Open House for EU Embassies coordinated by the Office of International Affairs. The Open House provided EU Embassy officials with additional insight into the functions of the NTC, especially concerning PNR data, and provided information on DHS privacy protections imbedded in the U.S. – EU PNR Agreement; and
- participating in an NTC briefing and tour for Hungarian Minister of Interior Sandor Pinter and U.S. Ambassador to the EU William Kennard. The briefing and tour were intended to give the participants greater insight into DHS policies and practices in preparation for renegotiating the 2007 U.S. – EU PNR Agreement.

Travel was conducted in support of the U.S – E.U. PNR Agreement.

- The Chief Privacy Officer traveled to Lithuania, Latvia, Estonia, and Finland in October 2010 to conduct outreach on the Agreement, where she met with Ministries of Justice, Interior and Foreign Affairs, and with data protection authorities and the press.
- While in Brussels on September 21-23, 2010, the Chief Privacy Officer held bilateral meetings with European Commission and Belgian, French and British officials to discuss privacy, PNR and the overarching U.S. – EU data protection and privacy agreement.
- The Chief Privacy Officer and the IPP Director traveled with the Deputy Secretary for PNR Agreement negotiations on four separate occasions (three trips and one trip, respectively).

Additional outreach conducted in support of the U.S – E.U. PNR Agreement includes the following.

- on December 2, 2010, the Privacy Office's IPP and the Compliance Directors briefed three French government officials on privacy best practices in the DHS PNR program in connection with standing up a French PNR system.

- on April 13, 2011, the European Institute held a transatlantic roundtable in Washington, DC on homeland security with members of the European Parliament's LIBE Committee titled "Strengthening Civil Liberties & Security: EU-U.S. Cooperation on Data Protection, PNR and SWIFT." The Chief Privacy Officer gave the keynote address and participated in a panel discussion on data protection and information sharing with the EU.

Preventing and Combating Serious Crimes (PCSC) Agreements – The DHS Privacy Office provided subject matter expertise to the U.S. government negotiating team during several PCSC negotiations this year.

- From November 28 – December 2, 2010, the IPP Group Director travelled with the Visa Waiver Program Office to Japan to discuss aspects of the Japanese PCSC Agreement. She briefed the Japanese delegation on the U.S. privacy framework and DHS privacy policies.
- On April 29, 2011, the IPP Director briefed a Taiwanese PCSC delegation in conjunction with the Visa Waiver Program Office's discussions to address privacy protections in the agreement.

U.S. – EU Data Protection and Privacy Agreement (DPPA) – The Privacy Office participates in the interagency team with the Departments of State, Justice, and Treasury, to negotiate the U.S. – EU DPPA.

- On December 9, 2010, the Deputy Chief Privacy Officer and the IPP Director met with three officials from the UK Ministry of Justice (MOJ) Human Rights and International Directorate. The UK MOJ officials requested the meeting to discuss their approach to the forthcoming negotiations on the European Commission's Directive for an umbrella data privacy agreement with the U.S. and to learn about data protection and data sharing initiatives under the Obama Administration.
- On January 25-28, 2011, the Deputy Chief Privacy Officer traveled to Belgium and Hungary for initial discussions on the DPPA, to attend the Justice and Home Affairs Ministerial and to speak on U.S. public sector privacy at the Data Protection Conference.

Canadian Discussions

- On June 13-14, 2011, the IPP Director traveled to Ottawa, Canada to serve as a subject matter expert for the Beyond the Border Working Group, and led discussions with Canadian colleagues on language for the U.S.-Canada Statement of Privacy Principles Terms of Reference.

2. Educational Outreach

The DHS Privacy Office contributed to a U.S. Mission to the EU-hosted seminar for U.S. law enforcement attachés, public affairs officers and global affairs officers posted in Europe on September 22-23, 2010, in Brussels. The Chief Privacy Officer and the IPP Director joined State and Justice Department officials to discuss transatlantic data privacy issues and the evolution of privacy as a foreign policy issue. The seminar provided foundational privacy awareness training and prepared officials with responses to expected challenges from EU Member States.

During the reporting period, the Privacy Office spoke at numerous domestic and international events, including events hosted by the U.S.-EU Justice and Home Affairs Ministerial, the

German Marshall Fund, and foreign embassies, and had meetings with EU and European Parliament representatives, members of the EU's Article 29 Working Party, and EU Member State ministries both in the U.S. and abroad. The Chief Privacy Officer and the Deputy Chief Privacy Officer were panelists at the widely attended International Conference of Data Protection and Privacy Commissioners Conference held in Jerusalem in October 2010.

Raising DHS Awareness on International Privacy –The IPP Director presented on international privacy issues, the role of U.S. privacy law, and DHS privacy policy to US-VISIT and USCIS staff, during their respective privacy weeks.

DHS Secure Flight Program – The Chief Privacy Officer made recommendations to the Chair of the standing Committee on Transportation, Infrastructure and Communities in Canada's Parliament regarding an amendment to its aviation law to allow Canadian airlines to share personal information with DHS for overflights of U.S. airspace. The purpose of these recommendations was to correct inaccuracies regarding options for Canadian citizens to seek access and redress that were submitted to Parliament by Canada's Privacy Commissioner. The Canadian Parliament subsequently amended the Canadian aviation law providing airlines with assurance they could comply with both Canadian and U.S. law.

U.S. Embassy Ottawa Briefing – The DHS Privacy Office participated in a briefing for outgoing U.S. Embassy officials discussing its responsibilities within the Department and explaining potential misperceptions held by Canadian counterparts regarding U.S. privacy law and DHS privacy policies and practices.

Europe – DHS has a number of ongoing initiatives with European Union multilateral organizations and with individual EU Member States. To build cooperation and maintain consistency across the region, the DHS Privacy Office participates in various DHS transatlantic working groups, including:

- The U.S. – EU Justice and Home Affairs Ministerial;
- U.S. – Germany Security Contact Group;
- U.S. – United Kingdom Joint Contact Group;
- Council of Europe; and
- the International Conference of Data Privacy and Protection Commissioners.

These fora enable the Privacy Office to share DHS privacy best practices as well as to mitigate privacy questions or concerns, identify DHS systems that collect or share PII with foreign partners, and ensure compliance with U.S. law and other international commitments.

Appendix III – Supplemental Component Information

A. NPPD

1. NPPD Overview

The NPPD Office of Privacy was established in August 2010 with the selection of the Senior Privacy Officer, who has developed close, collaborative working relationships among the leadership and staff of the DHS, NPPD, and US-VISIT privacy offices. This ensures effective implementation of privacy policies in furtherance of NPPD's commitment to safeguarding PII and sustaining and enhancing privacy protections for all individuals while promoting transparency, public participation and collaboration in support of the NPPD mission.

The offices of NPPD include:

Federal Protective Service (FPS): FPS is a proactive Federal law enforcement agency that provides integrated security and law enforcement services to federally owned and leased buildings, facilities, properties and other assets.
Office of Cybersecurity and Communications (CS&C): CS&C has the mission of assuring the security, resiliency, and reliability of the nation's cyber and communications infrastructure.
Office of Infrastructure Protection (IP): IP leads the coordinated national effort to reduce risk to our critical infrastructure posed by acts of terrorism. In doing so, the Department increases the nation's level of preparedness and the ability to respond and quickly recover in the event of an attack, natural disaster, or other emergency.
Office of Risk Management and Analysis (RMA): RMA serves as the Department's Executive Agent for national risk management and analysis.
US-VISIT: US-VISIT uses innovative biometrics-based technological solutions, digital fingerprints and photographs, to provide decision-makers with accurate information when and where they need it.

Although NPPD's overall mission is to reduce risk, each of the offices within NPPD operates under its own specific mission. The NPPD Office of Privacy engages each of the offices to ensure that the privacy program's mission is fully integrated into the organization's efforts to protect and secure PII. The Office of Privacy must also engage externally with the DHS Privacy Office and privacy offices in other DHS components to ensure overall consistency in how privacy is implemented throughout DHS.

2. US-VISIT Program

US-VISIT is a component within NPPD that provides biometric and biographic identity verification and analysis services for DHS components, federal agencies, and state and local law enforcement. US-VISIT maintains databases that store and share biometric information, such as fingerprints and digital photos, as well as certain biographic information. US-VISIT provides accurate and actionable information to those within DHS who are responsible for deciding eligibility for immigration benefits or admissibility into the United States, taking law enforcement actions, or granting access rights to sensitive facilities. In addition to DHS components, other users of US-VISIT's capabilities include federal agencies, state and local law enforcement, the intelligence community and international entities.

US-VISIT is the sole sub-component within NPPD that has its own privacy program, which predates the establishment of the NPPD Office of Privacy.

The mission of the US-VISIT Privacy Office is to uphold the privacy of individuals while helping to protect our nation. The Office accomplishes its mission by adhering to U.S. privacy laws, complying with the FIPPs, treating people and their personal information with respect, and ensuring a high standard of privacy protection.US-VISIT has a dedicated privacy officer who oversees privacy practices and works to protect information from misuse. Privacy is integrated into US-VISIT from conception through the planning, development, and execution of every aspect of the program.

3. Other Privacy Awareness Activities

- In August 2010, US-VISIT Today (a daily US-VISIT online newsletter) ran a privacy message on safeguarding PII for one week.
- In September 2010, the NPPD Office of Privacy began distributing its Safeguarding Sensitive PII Fact Sheet to all NPPD employees and contractors during classroom training events.
- In March 2011, US-VISIT Privacy worked with the DHS FOIA Office on a message in US-VISIT Today reminding employees of Sunshine Week.
- In April 2011, the US-VISIT Privacy team created a PTA Overview PowerPoint presentation to inform other US-VISIT branches of when and why the Privacy Office writes PTAs.
- In May 2011, US-VISIT Today ran a privacy tip to remind all US-VISIT employees how to safeguard their information and prevent identity theft.
- In June 2011, NPPD launched a page on the Department's intranet site, DHSConnect, to serve as a one-stop shop for privacy information affecting the NPPD community.

B. S&T

As discussed in Part One, Section VIII.F, the S&T Privacy Office worked on a number of PIAs and SORNs during this reporting period. The following provides more details about some of them. S&T:

- completed the Volunteers PIA for research projects that involve volunteer participants. The publication of this PIA improved efficiency by significantly reducing the amount of time S&T Program Managers needed to devote to privacy compliance requirements. This PIA covers 35 projects, including:
    - The Systems Assessment and Validation for Emergency Responders (SAVER) Simulator program, which routinely works with the emergency responder community to conduct tests and evaluations on responder technologies. The PIA provides a privacy protective framework for SAVER, to ensure that the program is protecting the privacy of individuals who volunteer in these studies; and
    - The Bomb End Cap Testing project that tests and evaluates bomb-end cap removal robots used by bomb squads in real-world operational scenarios.

  - The First Responders Coping Mechanisms for Post-Traumatic Stress Disorder (PTSD) project that aims to identify and understand mechanisms that help first responders cope with job-related stress and avoid developing PTSD.

- completed the PIA for Biodefense Knowledge Management System 2.0, which is a tool that integrates existing, publically available bio-defense related data with user-provided law enforcement or intelligence data, enabling law enforcement or intelligence users to conduct topic-based searches and find intersections between data sources;
- completed the PIA for the Transportation Security Laboratory (TSL) Biometrics Access Control System (BACS). TSL is a building access control system that uses biometric identifiers (iris images and fingerprint data) to identify authorized TSL personnel; and
- collaborated with the DHS Office of Health Affairs to publish the Contractor Occupational Health and Immunization SORN. This SORN covers the collection of contractor health records as part of S&T's occupational health surveillance operations.