DHS Privacy Office

Annual Report to Congress

July 2009 – June 2010

September 2010

Homeland Security

Message from the Chief Privacy Officer

The DHS Privacy Office is proud to present its sixth Annual Report covering the time period from July 2009 through June 2010. This report, as well as previous reports, can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

I have had the privilege of serving as the DHS Chief Privacy Officer for over one year now, and am heartened at the great strides the DHS Privacy Office has made in enhancing privacy protections within the operations of the Department while concurrently fulfilling the Administration's goals of transparency, public participation, and collaboration. The DHS Privacy Office continues to cultivate a true culture of privacy within the Department. Our efforts over the last year have borne significant fruit. For example, as of the close of the reporting period there are full-time, senior privacy officers in all of the operational components, and privacy officers for the National Protection and Programs Directorate and the DHS Intelligence and Analysis component, respectively, will have come on board as of this Report's release. 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 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 the operations of the Department. 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 merged in a manner that keeps this country safe and honors the principles on which the country was founded.

In that spirit, we also actively lead privacy policy development across the federal government both through leadership positions in all of the federal privacy organizations and through ongoing policy work in those organizations. When issues arise that affect the federal government as an enterprise, DHS Privacy Office staff utilizes any opportunity to be a voice for privacy protections, and has 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 intense 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 advice on interpreting international privacy legislation and 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 Department of Homeland Security Privacy Office (DHS Privacy Office or Office) is the first statutorily created privacy office in any federal agency, as set forth in Section 222 of the Homeland Security Act, 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 privacy and international community. 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 across the Department;
- Advancing privacy protections throughout the federal government through active participation in interagency fora;
- Conducting outreach to the Department's international partners to promote understanding of the U.S. privacy framework generally and the Department's role in protecting individual privacy; and
- Ensuring transparency to the public through published materials, reports, formal notices, public workshops, and meetings.

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. The continued leadership of the DHS Privacy Office is exemplified in many areas.

Within DHS, the DHS Privacy Office has:

- Supported designation, hiring, and development of full-time component privacy officers throughout the Department.
- Approved and published 79 Privacy Impact Assessments (PIAs), 31 System of Records Notices (SORNs) and entered into four Computer Matching Agreements.
- Developed a compliance and policy framework to address the privacy issues associated with the Department's use of social media, once again setting the standard for how the Department and other agencies embrace this technology.
- Revised its *Privacy Impact Assessment Official Guidance*, which is designed to examine the various requirements of the E-Government Act and Homeland Security Act and to guide the process of completing a PIA. This seminal publication has become the model used by many other federal agencies.

[1] 6 U.S.C. § 142.

- Initiated Privacy Incident Handling quarterly meetings to enhance privacy incident management, mitigation, and prevention across DHS components.
- Issued the *DHS Privacy Office Guide to Implementing Privacy* to educate the Department, other federal agencies, and the public about the DHS Privacy Office and provide transparency into Office functions and operations.
- Continued to provide training for DHS intelligence professionals assigned to state and local fusion centers as required in the Implementing Recommendations of the 9/11 Commission Act of 2007.
- Initiated a three-pronged approach to training state and local fusion center representatives, in cooperation with the DHS Office for Civil Rights and Civil Liberties, including a two-day "train the trainer" course for fusion center privacy officers taught at four regional fusion center conferences, in-person training for staff at seven fusion centers, and a Web-based resource toolkit.
- Commenced reviews of fusion center privacy policies on behalf of the Program Manager-Information Sharing Environment to ensure they are "at least as comprehensive" as the ISE Privacy Guidelines.
- Accepted additional new duties reviewing approximately 300 Intelligence and Analysis analytical products and 670 Homeland Intelligence Reports for privacy implications.
- Provided subject matter expertise on numerous international information sharing policies and agreements.
- Coordinated the processing of approximately 160,000 FOIA requests during the most recent FOIA reporting year and worked with component leadership to ensure adequate FOIA resources were available to address both backlog and incoming FOIA requests.
- Issued a memorandum to ensure the Department acts in accordance with President Obama's commitment to government transparency and proactive disclosure requirements, and posted more documents to DHS FOIA Reading Rooms to reduce routine FOIA requests.
- Improved the Office's website to provide more user friendly public access to Department PIAs, SORNs, and DHS Privacy Office guidance and reports.

In the Federal Community, the DHS Privacy Office has:

- Played a leading role in interagency development and implementation of privacy policy in the areas of cybersecurity and social media, and remains engaged in dynamic discussions related to cloud computing and online identity management.

Internationally, the DHS Privacy Office has:

- Participated in a multitude of international fora to increase international awareness of the Department's privacy policies and practices and to influence the international dialogue on privacy protection policies.
- Worked to raise awareness of Department and interagency personnel on the emergence of privacy as a foreign policy issue and the importance of educating foreign partners on U.S. privacy policies and practices.

As we move into a new era of open government and increased use of technology in government functions, the DHS Privacy Office will continue to diligently assess emerging issues and lead the way in establishing a more privacy-protective, open, and globally engaged government. This report details the DHS Privacy Office's leadership activities and initiatives during this reporting period in each of these areas.

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

Background

A. About the Office

The DHS Privacy Office (DHS Privacy Office or Office) is the first statutorily mandated privacy office in the federal government. Its 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. The Office works to minimize the impact of Department operations on an individual's privacy, particularly an individual's personal information and dignity, while achieving the Department's mandate. The Chief Privacy Officer reports directly to the Secretary of Homeland Security, and the Office's mission and authority are founded upon the responsibilities set forth in Section 222 of the Homeland Security Act of 2002 (Homeland Security Act), as amended.[2] Specifically, the Homeland Security Act created the Chief Privacy Officer at DHS with responsibilities to ensure privacy and transparency in government are implemented throughout the Department.[3]

Not only does the DHS Privacy Office serve as the steward of Section 222 of the Homeland Security Act, it also ensures that the Department complies with the Privacy Act of 1974,[4] the Freedom of Information Act (FOIA),[5] the E-Government Act of 2002 (E-Government Act),[6] and the numerous laws, Executive Orders, court decisions and Departmental policies that protect the collection, use, and disclosure of personal and Departmental information.

The Privacy Act of 1974 embodies a code of fair information principles that govern the collection, maintenance, use, and dissemination of personally identifiable information (PII) by federal agencies. The DHS Privacy Office's privacy compliance policies and procedures are based on the Fair Information Practice Principles (FIPPs), which are rooted in the tenets of the 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.*[7] The FIPPs inform the appropriate use of PII at the Department.[8] Application of the FIPPs enhances privacy protections by assessing the nature and purpose of all PII collected, and by ensuring that information fulfills the Department's mission to preserve, protect, and secure

[2] 6 U.S.C. § 142.
[3] Congress expanded the authorities and responsibilities of the Chief Privacy Officer in 2007 in the Implementing the Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) [Public Law 110-53]. Section 802 of the 9/11 Commission Act added investigatory authority, the power to issue subpoenas, and the ability to administer oaths, affirmations, or affidavits necessary to investigate or report on matters relating to responsibilities under section 222 of the Homeland Security Act. 6 U.S.C. § 142. These responsibilities are further described on the DHS Privacy Office website: http://www.dhs.gov/xabout/structure/editorial_0510.shtm and in Section 4 of the previous Annual Report available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf.
[4] 5 U.S.C. § 552a.
[5] 5 U.S.C. § 552.
[6] Pub. L. No. 107-347, 116 Stat. 2899.
[7] Available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[8] The FIPPs are set out in Appendix A.

the homeland. Thus, the DHS Privacy Office applies the FIPPs to the full breadth and diversity of information and operations within DHS. **Figure 2** illustrates how the FIPPs serve as a foundational framework for the DHS Privacy Office's varied efforts to foster a culture of privacy throughout the Department.

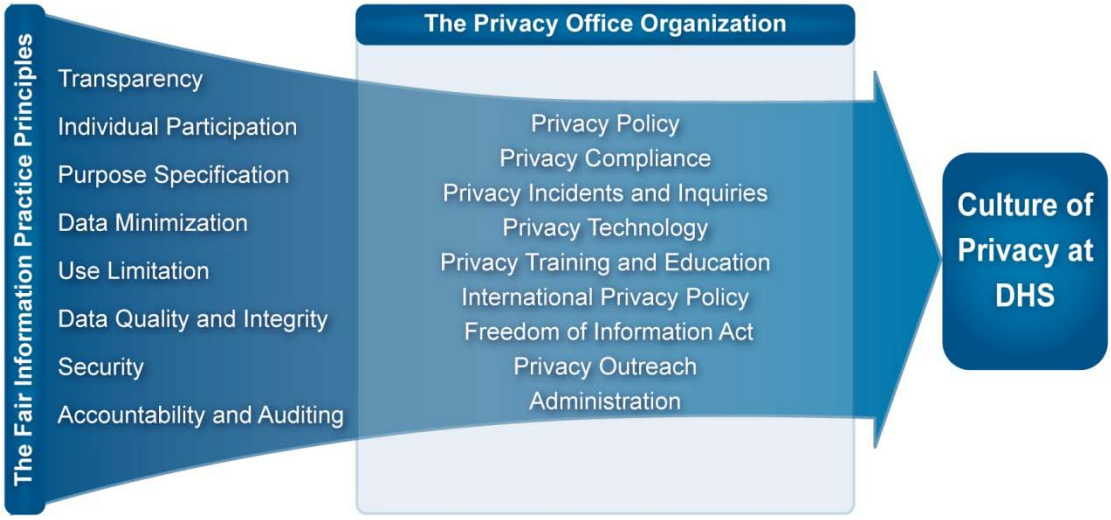


Figure 2: DHS Privacy Office Overview

FOIA implements the principle that persons have a fundamental right to know what their government is doing. Due to the symbiotic relationship between privacy and FOIA, the Chief Privacy Officer is also the Chief FOIA Officer for the Department. The E-Government Act mandates Privacy Impact Assessments (PIAs) for all federal agencies when there are new collections of, or new technologies applied to, PII.

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),[9] 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 operational implementation within the DHS components, 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;

[9] 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.

- 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 contributes to the Department's mission by ensuring that the Office is adequately staffed to support the increasing responsibilities and coordination required. In Fiscal Year (FY) 2010, the DHS Privacy Office received an appropriation of $7.971 million, an increase of $1.2 million (15%) over FY 2009.[10] As of July 2010, the Office staff includes 39 full-time equivalents, including one DHS Fellow and two interns.[11] The DHS Privacy Office is also supported by eight contractors. During FY 2010, the DHS Privacy Office added the following new personnel:

- FOIA Specialist (6)
- Privacy Compliance Specialist
- Attorney-Advisor
- Administrative Specialist
- Senior Privacy Analyst
- Privacy Analyst (2)
- Associate Director for Compliance (2)
- Associate Director of Communications and Training

By the time this report is published, a new Director of Privacy Policy and Senior Advisor will have joined the Office to replace Toby Levin, who retired in March after 25 years of federal service.

During the reporting year, the DHS Privacy Office converted contractor resources to recruit six FOIA Program Specialists to augment the current federal FOIA staff. DHS receives the largest number of FOIA requests of any department in the federal government. When DHS was established in 2003, it had the largest FOIA request backlog in the federal government. The

[10] The reporting period for this report runs from July through June, while the Department's fiscal year runs from October through September.

[11] The Office of Policy Honors Fellowship (DHS Fellow) is designed to develop the next generation of leadership within the U.S. Department of Homeland Security. Fellows are recruited from the nation's top graduate programs for a two-year appointment with three eight-month rotations throughout DHS. Through the rotational aspect of the fellowship, Policy Honors Fellows gain a broad understanding of DHS's mission and challenges, while components benefit from having Office of Policy employees and future leaders attuned to their perspective and mission.

additional FOIA staff enabled the DHS Privacy Office to handle the high volume of FOIA and Privacy Act requests and to provide support to DHS components as needed.

The Office is working closely with the DHS Office of Financial Operations, within the Office of the Chief Financial Officer, to convert additional contractor resources, with the goal of hiring an Associate Director of Privacy Incidents and Inquiries, a FOIA Program Specialist, a Privacy Program Analyst, and a Program Support Assistant in the future.

The DHS Privacy Office received a Biennial allocation to recruit a career Senior Executive Service Deputy Chief FOIA Officer in FY 2010 to serve as the key adviser to the Chief Privacy Officer and other senior DHS leadership on compliance with FOIA, the Privacy Act, and other DHS authorities, policies, programs, and agreements that promote government transparency and accountability.

The DHS Privacy Office will continue to promote growth in component privacy programs to address privacy requirements and enhance the culture of privacy throughout DHS. Component privacy staffing and support is discussed in Part One, Section IX of this report.

C. About this Report

This is the DHS Privacy Office's sixth Annual Report to Congress, covering the period July 1, 2009 through June 30, 2010. 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 Annual Report discusses the DHS Privacy Office's and DHS components' ongoing leadership in operationalizing privacy throughout the Department and across the federal government. It begins with an update on the appointment of privacy officers in the DHS components. It then describes the DHS Privacy Office's work in privacy compliance, privacy incident response, privacy oversight of DHS intelligence-related activities, and the Department's use of technology, and development of DHS privacy policy. It continues with a description of the DHS Privacy Office's central role in privacy policy development among other executive 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 Annual Report describes the DHS Privacy Office's significant 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. Part Two 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. The section 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 Annual Report provides an overview of the intensive 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. It also describes the DHS Privacy Office's leadership in mitigating the privacy implications of international agreements and its advice on interpreting international privacy frameworks.

The Annual Report concludes with a brief look into activities of the DHS Privacy Office going forward into the next reporting year.

Part One – Leading the Way: Operationalizing Privacy Protections

The diversity, complexity, and importance of the DHS mission require that the DHS Privacy Office excel on all fronts. The Office's clear mandate is to lead the charge in establishing privacy protections, advocating best practices, and promoting a culture of privacy at DHS. In addition, the Department's significant profile in the federal community demands that the DHS Privacy Office be a leader in advancing privacy across the federal government. In the past year, the DHS Privacy Office has proved itself more than equal to the challenge. From driving DHS privacy compliance mechanisms within DHS, to developing privacy guidance, policies and training, to directing the interagency privacy policy dialogue, the DHS Privacy Office has continued to provide privacy leadership and expertise to ensure privacy protections across the federal government.

I. Designation of Component Privacy Officers

In June 2009, the Deputy Secretary of Homeland Security issued a memorandum directing certain components to designate a senior level federal employee as a component privacy officer to serve as the primary point of contact for the DHS Privacy Office on privacy matters affecting the component. All of the following operational components have a privacy officer in place:

- Federal Emergency Management Agency (FEMA)
- Transportation Security Administration (TSA)
- U.S. Citizenship and Immigration Services (USCIS)
- U.S. Coast Guard (USCG)
- U.S. Customs and Border Protection (CBP)
- U.S. Immigration and Customs Enforcement (ICE)
- U.S. Secret Service (USSS)

As of June 30, 2010, the National Protection and Programs Directorate (NPPD) and Office of Intelligence and Analysis (I&A) had selected privacy officers, pending security clearance for the selectee. NPPD's and I&A's privacy officers will have entered on duty as of this Report's release. The Science and Technology Directorate (S&T) is actively recruiting a privacy officer.

Component privacy officers serve as first-line privacy authorities on privacy issues related to their respective components' collection, use, sharing, and retention of PII. Their privacy responsibilities include:

- Maintaining an ongoing review of all component Information Technology (IT) systems, technologies, rulemakings, programs, pilot projects, and other activities to identify collections and uses of PII and to identify any attendant privacy impacts.
- Coordinating with relevant component system managers and program managers, together with the Chief Privacy Officer and component counsel, to complete required privacy compliance documentation, including Privacy Threshold Analyses (PTAs), PIAs, and System of Records Notices (SORNs).
- Overseeing component implementation of all guidance documents and memoranda issued by the Chief Privacy Officer.
- Providing the Chief Privacy Officer all component information necessary to meet the Department's responsibilities for reporting to Congress or the Office of Management and Budget (OMB) on DHS activities that involve PII or otherwise impact privacy.
- Notifying the Enterprise Operations Center (EOC), the Chief Information Officer (CIO), the Chief Information Security Officer (CISO), the Chief Security Officer (CSO), the Component Computer Security Incident Response Center, and the Chief Privacy Officer about all potential or actual privacy incidents and overseeing the component's implementation of the guidance issued by the Chief Privacy Officer for handling such incidents.
- Processing privacy complaints from organizations and individuals, whether received directly or by referral from the Chief Privacy Officer.
- Overseeing component privacy training and providing educational materials, consistent with mandatory and supplementary training developed by the Chief Privacy Officer.
- Maintaining an ongoing review of all component data collection forms, whether electronic or paper-based, to ensure compliance with Privacy Act Statements and all implementing regulations and guidelines.

The appointment of component privacy officers expands and operationalizes the culture of privacy throughout the Department. DHS is the only federal agency to have senior federal privacy officials in each of its components, demonstrating DHS's commitment to privacy and to implementing Department-wide privacy protections.

II. Compliance Activities

The DHS Privacy Office Compliance Group (Compliance Group) is responsible for privacy implementation across DHS. The Compliance Group, which is led by the Director of Compliance, supervises the completion and approval of all PTAs, PIAs, and SORNs throughout DHS and thus plays a key role in providing the public transparency into Department systems and programs. In addition, the Compliance Group is responsible for meeting statutory requirements such as Federal Information Security Management Act of 2002 (FISMA)[12] 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, and other compliance reviews, and for conducting outreach to the component privacy officers and PPOCs to ensure privacy compliance requirements are met.

During this reporting period, the Compliance Group:

- strengthened the DHS compliance network and relationships with component privacy officers and PPOCs;
- developed and issued the *Comprehensive Compliance Template* and *Guidance Review and Update*;
- reorganized the Department's Data Integrity Board (DIB) and established a formal process for developing, reviewing, and processing computer matching agreements (CMAs) required under the computer matching provisions of the Privacy Act;
- expanded Compliance Group impact in the CIO's IT program reviews and in the Paperwork Reduction Act (PRA) process; and
- developed a compliance and policy framework to address the Department's use of social media.

The Compliance Group also hired two Associate Directors and has restructured itself to apply an increased focus on standardization and quality of compliance documentation and implementation of privacy compliance within the components. Aligning analysts with the Department's components and layering quality review by two Associate Directors as well as the Director of Privacy Compliance ensures that the Department's privacy compliance responsibilities are being consistently met. As the Compliance Group continues to mature, the component privacy officer and PPOC network expands, and privacy compliance becomes more embedded within the culture of DHS, the Compliance Group plans to focus on proactive reviews of DHS programs and systems to ensure they continue to meet standards set forth in the law and published privacy compliance documentation.

[12] 44 U.S.C. § 3544.

A. Building the Privacy Compliance Network

The DHS Privacy Office diligently works to develop a network to support privacy generally, and privacy compliance specifically, within DHS. Without this existing network, the privacy compliance process would be significantly hampered. The Chief Privacy Officer meets regularly with component privacy officers and PPOCs to address the importance of privacy, thus supporting the Compliance Group's efforts to strengthen privacy awareness and education and further bolstering the network of support for privacy.

During the reporting period, the Compliance Group continued to hold monthly meetings with component privacy officers and PPOCs to discuss compliance issues and areas of similar concern. These meetings serve a critical support function in coordinating and managing privacy efforts across the Department. Component privacy officers also began hosting the monthly compliance meeting to provide an overview and briefing of privacy activities and solutions within the host component. This new approach has provided an environment for component privacy officers and PPOCs to collaborate with each other, and with the Compliance Group, to discuss and address important privacy issues. Additionally, the Compliance Group continues to conduct quarterly off-site meetings with the component privacy officers and PPOCs to further strengthen the relationship between the component offices and the DHS Privacy Office. Component privacy officers and PPOCs discuss cross-cutting privacy issues, common privacy policies, and solutions during these quarterly meetings.

Outside of privacy channels, the Compliance Group also strengthened its relationship with other information-oriented offices such as the CIO, CISO, and Chief Financial Officer (CFO). This allowed the office to further expand the visibility of privacy compliance equities in the Department's existing and developing IT projects, initiatives, and systems and to bolster collaboration in the FISMA process, IT budget submissions, the EAB, the Program Review Board, and CIO IT program reviews.

B. Strengthening the Privacy Compliance Process

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. During the reporting period, the Compliance Group updated and reissued the DHS templates for all three documents to be more concise, self-explanatory, and transparent.

a. PTAs

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

b. PIAs

The use of PIAs is required by the E-Government Act and may also be invoked in accordance with the Chief Privacy Officer's statutory authority. PIAs have become an important tool for examining the privacy impact of IT systems, 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.

The PIA is the method by which the Compliance Group reviews system management activities in key areas such as security and how information is collected, used, and shared. 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. Part One, Section V.A.1 of this report discusses classified PIAs conducted during the reporting period.

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.[13] The DHS Privacy Office privacy compliance process depicted in **Figure 3** illustrates the iterative compliance documentation process.

[13] 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.

This continuous process enables the Compliance Group to regularly review both new and existing programs to ensure they continue to comply with privacy laws and regulations. Section 2 below describes each of these activities in greater detail.

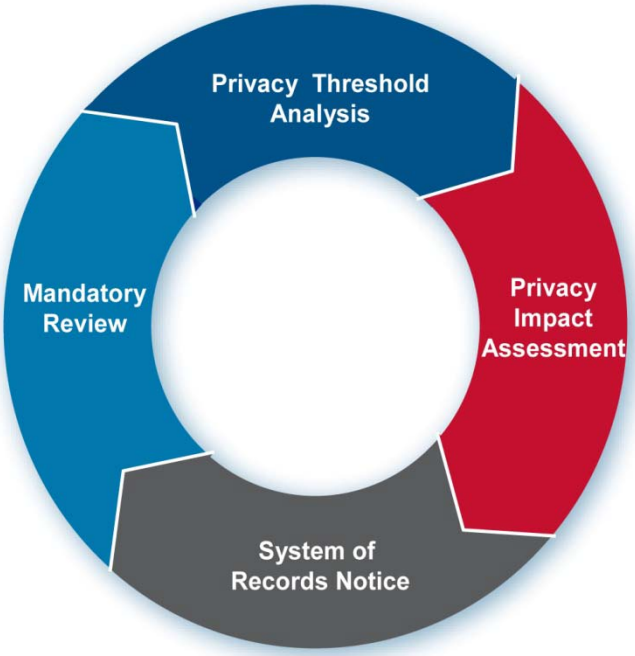


Figure 3: DHS Privacy Office Privacy Compliance Process

2. Compliance Template and Guidance Review and Update

Under the direction of the Chief Privacy Officer, the Compliance Group undertook a comprehensive review of its guidance and templates aimed at improving the quality and consistency of privacy compliance documentation for the Department. During this process, the Compliance Group sought advice and input from privacy experts including individual members of the Data Privacy and Integrity Advisory Committee (DPIAC), academia, component chiefs of staff, component privacy officers, and PPOCs. Updates reflect more mature compliance processes, increased focus on privacy analysis, and guidance within the templates to aid document preparers in meeting the Compliance Group's high standard. These updates benefit document users as well as consumers of the Department's privacy compliance documentation. These updates were rolled out on June 10, 2010 during the DHS Privacy Office's annual privacy compliance workshop. The workshop is discussed more fully in Part One, Section VIII.A.3 of this report.

a. PTAs

In November 2005, the Compliance Group pioneered the development of a new compliance tool, the PTA, and incorporated it into the Certification and Accreditation (C&A) process as a means of systematically assessing the privacy safeguards of IT systems. The PTA became mandatory in January 2006 for all IT systems, with a requirement that it be updated no less than every three years to coincide with the C&A process.

Since then, the PTA has developed into the mechanism by which the Compliance Group formally documents decisions for IT systems going through C&A, and those made by programs affecting privacy. For example, PTAs are now used to document and track rules affecting privacy, consistent with the DHS Privacy Office's mandate to conduct PIAs on proposed rules of the Department. In addition, PTAs are used to track information collections that are subject to the requirements of the PRA to ensure that such collections are appropriately covered by privacy

documentation and that a Privacy Act e(3) statement[14] is included on the form used to collect the information. The Compliance Group has refined PTAs for specific types of privacy sensitive initiatives or uses of PII that are common within the Department. These PTAs establish the rules that these initiatives and uses must abide by in order to be covered by enterprise-wide PIAs. For example, tailored PTAs have been created that allow programs to subscribe to DHS-wide PIAs established for contact lists and DHS web portals. This approach has reduced the number of individual PIAs that programs are required to complete while ensuring DHS programs use PII appropriately and consistently.

If a PTA identifies an IT system as a privacy sensitive system, the security requirements for the system confidentiality level are required to be designated as moderate, at a minimum, as stated in the *DHS Sensitive Systems Policy Directive 4300A* (DHS Directive 4300A).[15] By reviewing systems against the new PTA template, the Compliance Group obtains increased assurance that it is identifying those systems that are privacy sensitive. During the reporting period, the DHS Privacy Office reviewed and validated 540 PTAs.

b. PIAs

During the FY 2009 annual reporting period, the Compliance Group formalized its policy specifying when a PIA is required at the Department in its Privacy Policy Guidance Memorandum 2008-02, *DHS Policy Regarding Privacy Impact Assessments*.[16] 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 the use of the technology is high profile.
- **Pilot testing** when testing involves the collection or use of PII.

[14] 5 U.S.C. § 522a(e)(3).

[15] FISMA defines three security objectives for information and information systems: confidentiality, integrity, and availability. The National Institutes of Standards and Technology (NIST) Federal Information Processing Standards Publication 199 (FIPS-199), *Standards for Security Categorization of Federal Information and Information Systems*, prescribes standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. Agencies categorize their information and information systems according to FIPS-199 using low, moderate, or high for confidentiality, availability, and integrity, based on the potential impact on the agency should certain events occur which jeopardize the information and information its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[16] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf.

A compendium of PIA abstracts is published in the *Federal Register* (FR) on a periodic basis.[17] Between July 1, 2009 and June 30, 2010, the Chief Privacy Officer approved and published 79 PIAs. **Figure 4** illustrates the number of PIAs completed by each component during this reporting year.

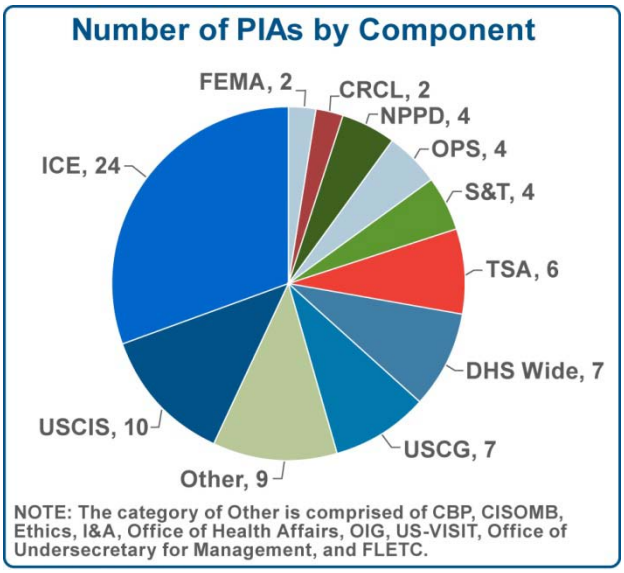


Figure 4: Number of PIAs Completed by Component during the Reporting Year

Another major accomplishment of the Compliance Group this year involved a thorough review and update of the PIA guidance and associated template. The Office reissued its *Privacy Impact Assessment Official Guidance*[18] designed to review the various statutory requirements of the E-Government Act and Homeland Security Act and to guide the process of drafting a PIA. This PIA guidance and the PIA template are used by the components and headquarters staff responsible for drafting PIAs for their programs and systems. Originally published in 2005 and revised most recently in June 2010, the Department's PIA Guidance has been used as a model by other federal agencies.[19]

Figure 5 depicts the percentage of DHS PIAs published in FY 2010 by type. A list of all PIAs published during the reporting period is provided in Appendix B. Examples of some of the more notable PIAs issued during the reporting period are discussed below.

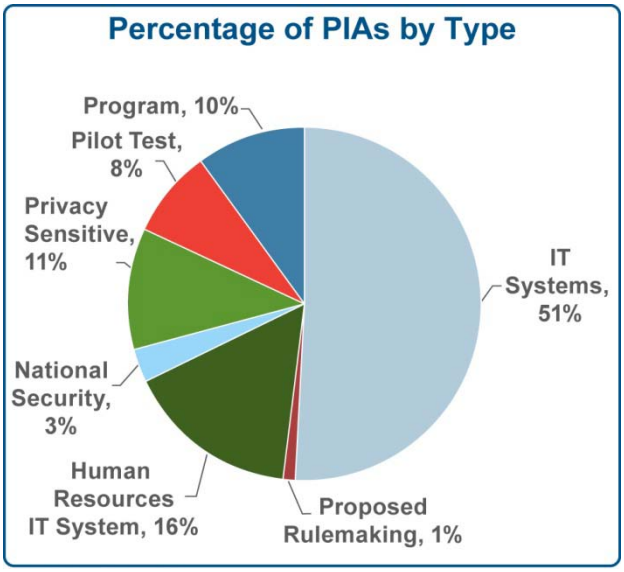


Figure 5: Percentage of PIAs Published during the Reporting Year by Type

Border Searches of Electronic Devices

The Compliance Group worked in concert with CBP and ICE to provide transparency into border searches of electronic devices through publication of a PIA. The PIA discusses advances in technology that have enabled the ability to easily and economically carry vast amounts of information in electronic form using compact, large capacity, and inexpensive electronic devices, such as laptop

[17] PIAs are posted at the following link on the DHS Privacy Office website: www.dhs.gov/privacy, then follow links to Privacy Impact Assessments.
[18] http://www.dhs.gov/files/publications/gc_1209396374339.shtm.
[19] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_june2010.pdf.

computers, thumb drives, compact disks, digital versatile disks, cell phones, subscriber identity module cards, digital cameras, and other devices. The contents of any such devices may be highly personal in nature. The PIA provides notice that such items and all other belongings, when carried by a traveler crossing the U.S. border, are subject to search by DHS to ensure the enforcement at the border of immigration, customs, and other federal laws. In particular, CBP and ICE may conduct border searches of such electronic devices as part of CBP's mission to interdict, and ICE's mission to investigate, violations of federal law at and related to the nation's borders. Part One, Section IX.A.1 of this report provides further discussion of the Border Searches of Electronic Devices PIA.

E-Verify Program

DHS published two PIAs related to the E-Verify Program, a service administered by the Verification Division of USCIS. E-Verify allows employers to electronically verify the employment eligibility of their newly hired employees. Previously, USCIS addressed the E-Verify program as part of the Verification Information System PIA. USCIS conducted a separate PIA for the E-Verify program in order to better assist the public in understanding this program. Further, USCIS conducted an update to the E-Verify PIA specifically to provide additional transparency into its use of commercial data for employer registration. This PIA provides transparency into the expanded information collection on registered employers participating in the E-Verify Program. The PIA describes the additional employer business information collected from both registering employers and a commercial data provider, Dun and Bradstreet (D&B), in order to enhance the employer registration process, manage customer relationships, and improve reporting capabilities and operational effectiveness. See Part One, Section IX.H for additional discussion on the E-Verify program.

Travel and Employment Authorization Listings

The Compliance Group worked with USCIS to provide transparency into the Travel and Employment Authorization Listings (TEAL) system through publication of a PIA. USCIS developed TEAL to streamline access to relevant information during the adjudication of certain benefits. TEAL consolidates immigration information about applicants from selected USCIS and DHS systems to provide greater accessibility to immigration information necessary to determine benefit eligibility. The PIA provides public notice regarding the IT systems TEAL retrieves information from as well as the uses of the information by USCIS adjudicators.

Recruit Analysis and Tracking System

DHS published a PIA for the Recruit Analysis and Tracking System (RATS), a system used by the U.S. Coast Guard (USCG) to support its recruiting mission. USCG conducted this PIA because RATS collects and retains PII from potential enlisted recruits and officer candidates. The PIA provides transparency into how the U.S. Coast Guard uses the system to gather and distribute recruiting leads, track recruit progression, prepare accession forms, and process reservations for enlisted and officer candidates. In addition, the PIA describes the uses of recruiting data for reporting functions on quality, quantity, and diversity statistics associated with the recruiting effort.

Coast Guard Academy Information System

DHS published a PIA for the Academy Information System (ACADIS), a system used by the U.S. Coast Guard Academy (CGA) for the management of the CGA educational environment

including the training and development of all future Coast Guard Officers. USCG conducted this PIA because ACADIS collects and maintains PII from CGA applicants, cadets, faculty, and staff. The PIA describes ACADIS functions including processing of transactional data for cadet military program records and various facility applications, management of applicant data to facilitate the admissions process, and warehousing of data on cadets, prior cadets, faculty, and staff.

Family Registry and Locator System

DHS published a PIA for the National Emergency Family Registry and Locator System (NEFRLS), operated by FEMA. NEFRLS is a web-based system which, when activated during a Presidentially-declared disaster or emergency, enables FEMA to provide a nationally accessible and recognized system that allows adults displaced from their home or pre-disaster residence to voluntarily register to facilitate the reunification of their family and household members (registrants). Individuals who are searching for displaced family or friends, or household members may also register in the system (searchers). FEMA conducted this PIA to describe the uses and controls placed on PII collected from registrants and searchers. Specifically it describes how registrants are authenticated to the system and provide limited PII on any household or family members traveling with them and identify up to seven individuals who they authorize to view their PII, including their current location and contact phone numbers.

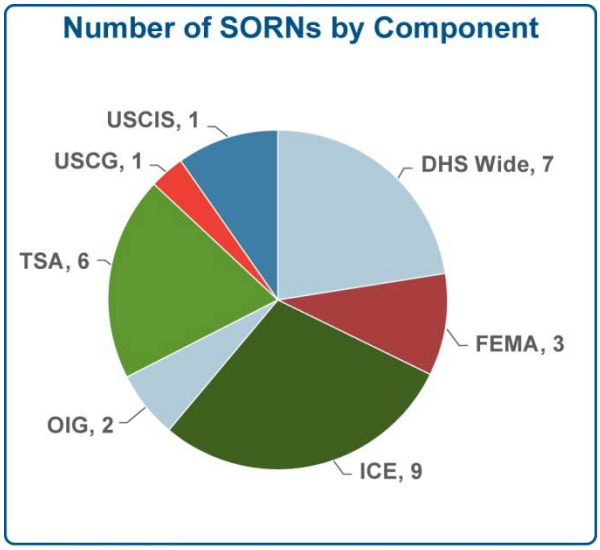


Figure 6: Number of SORNs Published by Component during the Reporting Year

c. SORNs

During the reporting period, the Chief Privacy Officer approved and published 31 SORNS. **Figure 6** depicts the number of SORNs published during the reporting year, by component. A complete list of published SORNs is provided in Appendix C. A few examples are discussed below.

- DHS/TSA-023, Workplace Violence Prevention Program – DHS/TSA developed this SORN to cover records regarding current and former employees and contractors of TSA and members of the public who have been involved in workplace violence at TSA facilities or while on, or because of, their official duty. This SORN also covers those individuals who are being or have been assisted or counseled by the TSA Workplace Violence Prevention Program. Records include acts, remarks, or gestures that communicate a threat of harm or otherwise cause concern for the safety of any individual at TSA facilities or while on or because of their official duty. These records may include identifying information, information documenting workplace violence, and actions taken by the Workplace Violence Prevention Program or TSA. DHS/TSA has exempted this system from the notification, access, and amendment procedures of the Privacy Act

because it is a law enforcement system. DHS/TSA will, however, consider individual requests to determine whether or not information may be released.

- DHS/ICE-001, Student Exchange Visitor Information System (SEVIS) – In conjunction with the development and launch of the next-generation SEVIS application, called SEVIS II, DHS/ICE modified its SORN to propose the collection of additional information on students, exchange visitors, and their dependents who are in the U.S. on F, M, or J classes of admission (F/M/J nonimmigrants), and information on officials of approved schools and designated sponsors of F/M/J nonimmigrants. Like its predecessor, SEVIS II is an information system that tracks and monitors F/M/J nonimmigrants throughout the duration of their approved participation within the U.S. education system or designated exchange visitor program.
- DHS/ALL-023, Personnel Security Management – DHS updated and reissued this SORN to include records systems within the Federal Protective Service and records of federal, state, local, and foreign law enforcement personnel who apply for and are granted authority to enforce federal laws on behalf of DHS. This SORN is the baseline system for personnel security activities, as led by the DHS Office of the Chief Security Officer, for the Department.
- DHS/ICE-012 Visa Security Program Records – The DHS ICE Visa Security Program Records (VSPR) system manages, reviews, tracks, investigates, and documents visa security reviews conducted by ICE agents pertaining to U.S. visa applicants to document ICE visa recommendations to the U.S. State Department. The system contains information about individuals who have applied for U.S. visas and who undergo a visa security review.
- DHS/ALL-001 FOIA and Privacy Act Records System – DHS published this SORN to update FOIA and Privacy Act Records System as part of the biennial review. The system collects and maintains records that concern the Department's FOIA and Privacy Act Records.
- DHS/FEMA-001 NEFRLS – NEFRLS provides a nationally accessible electronic system that allows adults displaced from their homes or pre-disaster location after a Presidentially-declared emergency or disaster to voluntarily register themselves, and to identify up to seven family or household members whom they authorize to access PII that may potentially include their current location or a special message to an identified individual. The system will allow individuals registered in the system and individuals who are searching for family or household members to reunite.

C. Computer Matching Agreements and the Data Integrity Board

Under the Computer Matching and Privacy Protection Act of 1988, which amended the Privacy Act, federal agencies must establish a DIB to oversee and approve their use of computer matching programs.[20] 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[21] and DIB members include the Inspector General and representatives of components that currently have active CMAs in place.[22]

Before the Department can match its data with data held by another federal 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.[23]

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 entered into:

- One 18-month CMA, formally establishing a computer matching program between FEMA and the Small Business Administration.
- One 18-month CMA, formally establishing a computer matching program between ICE and the Social Security Administration (SSA).
- One 18-month CMA, formally establishing a computer matching program between USCIS and the Department of Education.
- One 18-month CMA, formally establishing a computer matching program between USCIS and the SSA.

[20] 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).

[21] 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).

[22] The Inspector General is a statutory member of the Data Integrity Board. 5 U.S.C. § 552a(u)(2).

[23] 5 USC § 552a(o).

D. Additional Compliance Reporting and Oversight

In collaboration with the CIO, CISO, and CFO, the Compliance Group identifies programs that must go through the privacy compliance process through several avenues including: (1) the FISMA C&A process; (2) the OMB IT budget submission process; (3) the Enterprise Architecture Center for Excellence (EACOE) process; (4) CIO IT Program Reviews; and (5) 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. See Part One, Section VII.B for additional discussion on DHS Privacy Office activities with the CIO and CISO.

1. 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 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 third quarter FY 2009 reporting period, DHS had conducted PIAs on 55% of the IT systems that required PIAs. 93% of the IT systems were covered by a SORN. At the end of the reporting period, DHS's FISMA privacy numbers were 70% for PIAs and 93% for SORNs. ICE had the most improved PIA score for this time period, improving its PIA score from 30% in the third quarter of FY 2009 to 71% by the third quarter of FY 2010. ICE published 24 PIAs, making it the highest producer of PIAs among the components during the reporting period. ICE's accomplishment is one of the many tangible impacts realized by establishing a component privacy officer.

2. 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.[24] 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

[24] *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/OMBcirculars/a11/current_year/s300.pdf.

the Department's IT investments meet the established legal and policy standards set forth by DHS, OMB, and Congress.

During the FY 2011 budget review process,[25] the Compliance Group reviewed 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 ten IT investments through the OMB 300 scoring process due to insufficient privacy protections and privacy documentation.[26]

During this reporting period, the Compliance Group assisted three IT investments with resolving privacy issues by completing PIAs or SORNs: the NPPD Integrated Common Analytical Viewer Sensitive But Unclassified PIA,[27] the ICE Enforcement Integrated Database PIA,[28] and the Immigration and Enforcement Operational Records SORN.[29] At the end of the reporting period, the Compliance Group was in the process of the FY 2012 review.

3. Enterprise Architecture Board

As a means of ensuring that privacy is considered at the beginning of every IT development effort, the DHS Privacy Office sits on the EAB. The EAB operates through the Office of the Chief Information Officer (OCIO) and performs substantive and strategic reviews of all requests for new IT initiatives through its operational sub-organization, the EACOE. The DHS Privacy Office sits on the EACOE and reviews each request for new technology to ensure that the Department's use of technology sustains privacy protections.

4. Chief Information Officer IT Program Reviews

The Compliance Group continued to broaden the DHS Privacy Office's reach this year through participation in the CIO's IT program reviews for DHS's major IT investments. These program reviews were ordered by the new CIO, and as part of the standard briefing programs must demonstrate how they have met privacy compliance requirements. This is yet another mechanism the Compliance Group uses to identify privacy risks and assure technologies sustain and do not erode privacy protections. These briefings also provide the CIO and other high-level DHS officials with visibility into the Department's major investments and can serve as an opportunity to further the privacy agenda.

5. Paperwork Reduction Act 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

[25] The FY 2011 budget review process took place between June and August 2009.
[26] 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.
[27] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_icav.pdf.
[28] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_eid.pdf.
[29] http://edocket.access.gpo.gov/2010/2010-10286.htm.

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 is in regular contact with the PRA Program Management Office within OCIO.

6. Program Review Board

The Chief Privacy Officer has been 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, increase stability of the Future Years Homeland Security Program,[30] 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.

E. Compliance and Policy Framework to Address Social Media

The President's Transparency and Open Government Directive and related Memorandum[31] direct federal departments and agencies to harness new technologies to engage the public. DHS is planning to engage the public using social media in a variety of ways.[32] For example, the Department's use of the public engagement site, IdeaScale, provides an online platform to solicit ideas from the public and to enable the public to view, rate, and comment on other user-submitted ideas. The federal government's use of social media requires that legal, accessibility, privacy, communications, information security, and records management considerations be addressed prior to launching social media tools and activities. In support of this initiative, the Compliance Group has enhanced its capacity to analyze the privacy issues raised by the Department's use of social media initially through PTAs, PIAs, and SORNs to ensure that Department use of social media complies with the Privacy Act, Homeland Security Act, and E-Government Act.[33] The Compliance Group is also working with the Office of the General Counsel (OGC), Office for Civil Rights and Civil Liberties (CRCL), Office of Public Affairs (OPA), CISO, and Records Management, as a member of the Department's new media compliance steering committee, to comprehensively review policies, plans, and supporting documentation that will govern the use of social media at DHS. Additionally, the Compliance

[30] 6 U.S.C. § 454.
[31] 74 Fed. Reg. 4685 (Jan. 26, 2009), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf; 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.
[32] A list of all DHS social media initiatives can be found at http://www.dhs.gov/xabout/gc_1238684422624.shtm.
[33] The privacy compliance process will determine whether DHS Components are collecting, using, maintaining, or disseminating personally identifiable information and whether the activity triggers the Privacy Act's SORN requirement, as well as ensuring that the activity complies with PIAs that are under development.

Group actively participated on the Federal CIO Council Privacy Committee's Web 2.0 Subcommittee to develop social media SORN and PIA templates and the Privacy Committee's guidance for federal agency use.

Social Media PTAs

During this reporting period, the Compliance Group introduced the Social Media PTA to triage social media initiatives into specific categories that will then either be covered by DHS-wide social media PIAs or require drafting a new, more specific, social media PIA.

Social Media PIAs

The Compliance Group is developing enterprise-wide social media PIAs to cover the range of social media initiatives underway at the Department. These PIAs establish the rules under which specific categories of Department social media initiatives operate.

Also during this reporting period, the Chief Privacy Officer approved the following social media-related PIAs:

DHS-wide

Our Border Network – The Office of International Affairs (OIA) and CBP, in coordination with OPA, developed this PIA on the use of the social networking site Ning.com to facilitate the creation of a "civic network" focused on southwest border issues. To become a member of the DHS network hosted by Ning, individuals must be a member of Ning.com which requires the collection of certain PII.

IdeaFactory – The Office of the Under Secretary for Management developed this PIA on the Intranet web-based tool that uses social media concepts to enable innovation and organizational collaboration within DHS. IdeaFactory empowers employees to develop, rate, and improve innovative ideas for programs, processes, and technologies. This PIA was conducted because the site will collect limited PII on users submitting ideas.

National Dialogue for the Quadrennial Homeland Security Review – The Office of Strategic Planning developed this PIA on the National Dialogue on the Quadrennial Homeland Security Review (QHSR) to facilitate conversations between the DHS and homeland security stakeholders on an innovative web-based platform. The National Dialogue is an interactive process, building on the public's input over the course of three dialogues. The Department conducted this PIA because the participant feedback will be collected with limited PII.

Office of Operations Coordination and Planning

The Office of Operations Coordination and Planning (OPS), including the National Operations Center, has led several social media event monitoring initiatives to aid in providing situational awareness and establishing a common operating picture for the entire federal government, and for state, local, and tribal governments as appropriate. The purpose of this initiative is to ensure that critical disaster-related information reaches government decision makers consistent with Section 515 of the Homeland Security Act.[34] The Compliance Group closely coordinated with OPS, often under very short deadlines, to issue the necessary PIAs, including: (1) Haiti Social Media Disaster Monitoring Initiative (January 21, 2010); (2) 2010 Winter Olympics Social

[34] 6 U.S.C. § 321d(b)(1).

Media Event Monitoring Initiative (February 10, 2010); and (3) April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative (April 29, 2010).

These PIAs were superseded by the OPS Publicly Available Social Media Monitoring and Situational Awareness PIA (June 22, 2010), which is not associated with a specific event but contains specific rules and entails a dedicated privacy compliance review after an initial pilot.

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. The Director of Privacy Incidents and Inquiries and staff, known as the Incidents and Inquiries Group, direct the Privacy Incident Management program in collaboration with the DHS EOC, component privacy officers and PPOCs, and DHS management.[35] The Incidents and Inquiries Group works to ensure all incidents are properly reported and that mitigation and remediation efforts are appropriate for each incident.

A. DHS Privacy Incident Response Plan

The DHS Privacy Office ensures compliance with privacy policy to include development, revision, and integration of the privacy incident response program throughout the Department. During this reporting period, the DHS Privacy Office worked steadily to continue refining and enhancing the *DHS Privacy Incident Handling Guidance* (PIHG), the primary resource for privacy incident policy within DHS.[36] 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),[37] which is the foundation for the management 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 System 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.

During the reporting year, the DHS Privacy Office also continued to refine its privacy incident management program. The DHS Privacy Office is revising the PIHG as well as a more concise "desktop" version of the PIHG. Each of these documents, along with associated passages in the DHS CISO's Concept of Operations, DHS Directive 4300A, and DHS 4300A Handbook are

[35] The Incidents and Inquires Group also supervises reviews of privacy complaints, as discussed in Part Two, Section II.A of this report.
[36] http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.
[37] http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.

under current revision to align them with the updated OMB mandates, as well as to include a "lessons learned" section illustrating the best practices developed over three years of operation.

A total of 279 privacy incidents were reported to the DHS EOC during the reporting period. The majority of the incidents affected a small number of individuals and data, while a select few incidents involved larger amounts of data. Mitigation and remediation of each incident is coordinated among the DHS Privacy Office, EOC, component privacy officers and PPOCs, and Information Systems Security Managers. DHS investigated, mitigated, and closed 250 or 90% of the reported privacy incidents. Of those reported, 10% remain open. By comparison, during the previous reporting year, the Office mitigated and closed 77% of the reported privacy incidents, and 23% remained open. The average number of days during which an incident remained open decreased from 46 in the previous reporting period to 27. The decrease is due to the constant communication and collaboration among the many offices mentioned above.

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

Type of Incident[38]	Number of Incidents: July 1, 2009 to June 30, 2010	Number of Incidents: July 1, 2008 to June 30, 2009
Alteration/Compromise of Information[39]	239	296
Classified Computer Security Incident[40]	2	12
Investigation Unconfirmed/Non-Incident[41]	19	18
Malicious Logic[42]	0	4
Misuse[43]	10	15
Unauthorized Access (Intrusion)[44]	8	6
Probes and Reconnaissance Scans[45]	1	0
Total	***279***	***351***

Table 1: DHS Privacy Incidents Reported

The privacy incident handling process at DHS continues to evolve. This program has been emulated by various federal agencies throughout the federal government.

[38] The types of incidents are detailed in National Insitute of Standards and Technolgy (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.

[39] **Alteration/ Compromise of Information** includes any incident that involves the unauthorized altering of information, or any incident that involves the compromise of information.

[40] **Classified Computer Security Incident** includes any security incident that involves a system used to process national security information. None of these incidents involved a breach of a classified system; rather, the incidents involved classified data "spilled" on unclassified systems.

[41] **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.

[42] **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.

[43] **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.

[44] **Unauthorized Access/Intrusion** includes all successful unauthorized accesses and suspicious unsuccessful attempts.

[45] **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.

B. Investigative Activity

The 9/11 Commission Act expanded the Chief Privacy Officer's responsibilities to include explicit investigative authority, the power to issue subpoenas, the ability to conduct regular reviews of privacy implementation, and greater coordination with the Inspector General.[46] During the reporting period, the Chief Privacy Officer invoked this authority to initiate an investigation into a privacy incident that affected several components and triggered multiple privacy and security concerns. The investigation required coordination with several component agencies including the Office of the Inspector General; this coordination was critical to ensure proper mitigation occurred and to prevent the likelihood of a recurrence. At the end of the reporting period, the Director of Privacy Incidents and Inquiries was preparing a report with findings and recommendations that will address compliance with privacy policies regarding the proper collection, safeguarding, destruction, and transmission of PII. The report can be expected to recommend steps for proper mitigation and to prevent the likelihood of a recurrence. The Chief Privacy Officer anticipates conducting more investigations in the next reporting period. Thus, the capacity of the Incidents and Inquiries Group can be expected to grow. As of this report's release, the DHS Privacy Office anticipates recruitment of an Associate Director of Privacy Incidents and Inquiries to assist in complex privacy investigative matters.

C. Annual Core Management Group Meeting

OMB M-07-16 recommends, and DHS has implemented, a standing Core Management Group (CMG), a DHS executive management group that meets annually to evaluate and discuss privacy incidents and incident handling procedures. The DHS CMG includes the Chief Privacy Officer, DHS Leadership, component IT security entities, component privacy officers, and PPOCs.

In July of the reporting period, the Chief Privacy Officer hosted the inaugural meeting of the Privacy Incident Management Annual CMG Meeting. The 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 June 2009.

Following the meeting, the DHS Privacy Office published the CMG After Action Report, which summarized the CMG meeting. The group used the metrics to determine where incidents are occurring in order to target areas of vulnerability and to direct training, as appropriate, to prevent incidents. The CMG will continue its work with annually scheduled meetings.

[46] Congress expanded the authorities and responsibilities of the Chief Privacy Officer in 2007 in the Implementing the Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) [Public Law 110-53]. Section 802 of the 9/11 Commission Act added investigatory authority, the power to issue subpoenas, and the ability to administer oaths, affirmations, or affidavits necessary to investigate or report on matters relating to responsibilities under section 222 of the Homeland Security Act. 6 U.S.C. § 142.

D. Collaboration

1. Collaboration with Components

The Incidents and Inquiries Group collaborates with each component to monitor and manage privacy incidents. During this reporting year, the Incident and Inquiries 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. The Incidents and Inquiries Group also assisted the components in identifying privacy incident trends, discovering areas of vulnerability, and ultimately preventing the likelihood of future incident occurrences. The component visits also enabled the DHS Privacy Office to observe how the components incorporate privacy protections into all aspects of their mission. These collaborative visits will continue throughout the next reporting year to provide the remaining components the opportunity to raise potential issues and discuss resolutions in a collegial environment. The DHS Privacy Office is also developing training based on the lessons learned during these visits, which will lead to increased awareness and prevention of privacy incidents. Part One, Sections IV.A.2, V.A.2, and VIII of this report discuss the full breadth of DHS Privacy Office training activities conducted during this reporting period.

2. Collaboration with DHS EOC

Close communication with the EOC continues to provide a unique and open mechanism for managing an efficient and effective reporting system with a high level of trust between the DHS Privacy Office and EOC analysts in charge of the incident reporting process. For instance, the Incidents and Inquiries Group met with EOC personnel for a demonstration of their privacy incident management online tracking system. The visit strengthened the collaboration between the offices and yielded immediate improvements in creating a more efficient tracking system. As a result of the visit, a new queue system has been implemented which has decreased the amount of time an incident remains open. The DHS Privacy Office continues to monitor the reporting system and request modifications to the online reporting process to reflect lessons learned and new capabilities, and to obtain reporting capabilities that provide key metrics for the program. The DHS Privacy Office also participates in a weekly conference call to discuss issues related to incidents.

3. Collaboration with other Federal Agencies

In March 2010, the Deputy Chief Privacy Officer and the Incidents and Inquiries Group met with privacy officials from the Internal Revenue Service (IRS) for a thorough discussion, a demonstration of the IRS Privacy Incident Management Online Tracking System, and to share best practices. The visit allowed the staff of both agencies to learn more about the unique issues each agency faces pertaining to incident response given their respective office structures and missions.

E. Privacy Incident Handling Quarterly Meetings

Beginning this reporting period, the Director of Privacy Incidents and Inquiries initiated Privacy Incident Handling quarterly meetings to enhance the privacy incident handling program at DHS. The Incidents and Inquiries Group hosted Privacy Incident Handling Quarterly Meetings in November 2009, February 2010, and June 2010. These fora provided an opportunity for the

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. On two occasions, components have provided briefings on the unique issues they face.

F. Outreach and Training

During the reporting period, the Director of Privacy Incidents and Inquires presented an overview of the DHS Privacy Incident Response program to chief privacy officers and senior agency officials for privacy at the inaugural 2009 Federal CIO Council Privacy Committee's Chief Privacy Officer Boot Camp.[47] The Director also presented an informational briefing on two occasions to International Privacy Exchange visitors hosted by the DHS Privacy Office.

In September 2009, the Incidents and Inquires Group issued *Privacy Incident Guidance*, a DHS Privacy Office internal desktop reference. The Office provided the guidance to component privacy officers and PPOCs for their information and to use to develop their internal component policies. The Director also conducted training based on the guidance. The training is tailored for the DHS Privacy Office internal operations, providing practical tools for DHS Privacy Office employees to use if they encounter privacy incidents within the office or in other DHS components.

[47] The Boot Camp is described in Part One, Section VII.C of this report.

IV. Privacy in DHS Intelligence Activities

The DHS Privacy Office's oversight and support responsibilities are perhaps nowhere more critical than in the area of DHS intelligence activities. During the reporting year, the Office provided essential guidance in its reviews of I&A analytic products for privacy implications and in its reviews of state and local fusion center privacy policies. Together with CRCL, the Office continued to provide a comprehensive training regime for staff of fusion centers and for the DHS analysts stationed there. By bringing its expertise to bear in these efforts, the DHS Privacy Office worked to ensure that the Department executes its intelligence function in a privacy-protective manner.

A. Fusion Centers

The DHS Privacy Office continued its leadership in the DHS State, Local, and Regional Fusion Center Initiative, as codified in Section 511 of the 9/11 Commission Act. These efforts centered on governance, training, and oversight.

In addition, for the third consecutive year, the DHS Privacy Office had a strong presence at the National Fusion Center Conference, providing briefings to fusion center leaders, addressing a breakout session, conducting training sessions, and staffing a booth with the DHS Office for Civil Rights and Civil Liberties.

1. Governance – State and Local Program Office

On December 7, 2009, Secretary Napolitano directed the Department to unify its efforts to support state and major urban area fusion centers to "coordinate the Department's relationship with, and support to, fusion centers to ensure a collaborative approach to those centers by all DHS Components." Through the Office of Intelligence and Analysis, the Department assembled a series of working groups to enhance the efficacy of the Department's support for the fusion center program. The Secretary's instructions included charges that the Department:

- develop, promote, and sustain rigorous legal, privacy, civil rights, and civil liberties training and related support to state, local, and tribal representatives as well as Department personnel deployed to state and major urban area fusion centers; and
- encourage participation in the Information Sharing Environment (ISE) among and between federal agencies and state and major urban area fusion centers in order to bolster our homeland security.

The DHS Privacy Office had full membership in the efforts to coordinate DHS support to fusion centers and actively participated in furtherance of the goals discussed above. The Office also served as a co-chair of the privacy and civil liberties working group.

2. Training

a. DHS Analysts Assigned to Fusion Centers

The DHS Privacy Office continued to train intelligence analysts assigned to fusion centers, as required under Section 511 of the 9/11 Commission Act.[48] This training begins with the Office's *A Culture of Privacy Awareness* course, available to all DHS employees online or on a CD. Following successful completion of the course, the DHS Privacy Office conducts a two-hour guided course entitled: *Privacy Fundamentals for Fusion Center Professionals*, which covers:

- Privacy Fundamentals and the DHS FIPPs
- Information Sharing Authorities and Parameters
- Data Breaches, other Privacy Incidents, and Incident Reporting
- Intelligence Reporting and Privacy

This introductory training is supplemented throughout the year at various events. During the reporting year, for instance, DHS Privacy Office representatives addressed I&A fusion center representatives at both the I&A Field Rep Offsite in El Paso, Texas in September 2009, and at National Fusion Center Conference in New Orleans, Louisiana in March 2010.

b. Training for State and Local Fusion Center Personnel

Section 511(i)(6) of the 9/11 Commission Act requires the Department to ensure fusion centers provide "appropriate" privacy training "in coordination with the Chief Privacy Officer" for all state, local, tribal, and private sector representatives within each fusion center.

To implement this, the DHS Privacy Office teamed with CRCL to develop a three-pronged approach to ensure the greatest possible coverage and breadth of training opportunities:

- Train-the-Trainers – Under the *Information Sharing Environment Privacy Guidelines*, as well as the *Global Justice Information Sharing Initiative (Global) Fusion Center Baseline Capabilities* (Global's Baseline Capabilities), fusion center ISE participants are required to appoint a privacy and civil liberties official. The DHS Privacy Office and CRCL–in cooperation with the Program Manager for the Information Sharing Environment (PM-ISE)–developed a two-day training session to help fusion center privacy officials understand the scope and importance of their roles, and prepare them to develop and deliver their own state-specific training programs.
  During the reporting year, the DHS Privacy Office, in conjunction with CRCL, delivered this training to 60 fusion center privacy and civil liberties officials during the four Regional Fusion Center Conferences around the Country:
  - Western Region, Portland, Oregon – April 27-28, 2010
  - Southeastern Region, Montgomery, Alabama – May 18-19, 2010
  - Central Region, Minneapolis, Minnesota – May 25-26, 2010
  - Northeastern Region, Philadelphia, Pennsylvania – June 15-16, 2010[49]

[48] 6 U.S.C. § 124h(c)(4)(A).
[49] The sessions were well-attended, and the DHS Privacy Office anticipates needing only a single makeup session in Washington DC during the next reporting year to achieve 100% coverage.

Attendees were asked to develop and deliver privacy and civil rights and civil liberties training at their home centers within six months of their train-the-trainers session. In addition to providing materials developed for DHS Privacy Office training responsibilities, the Office and CRCL will continue to work with these privacy and civil liberties officers to develop and refine their own training curricula.

- In-Person Training – During the reporting year, the DHS Privacy Office traveled with CRCL to seven fusion centers in Phoenix, Arizona; Seattle, Washington; Boston, Massachusetts; Maynard, Massachusetts; Jefferson City, Missouri; Kansas City, Missouri; and Tallahassee, Florida, to deliver the *Privacy Fundamentals for Fusion Center Professionals* training course, which is adapted from the training provided for I&A personnel. This training is meant to complement – not replace – the comprehensive, state-specific training delivered by each fusion center's privacy officials. The pace of these in-person sessions slowed down while the DHS Privacy Office and CRCL developed and delivered the train-the-trainer classes, but both offices are in the process of scheduling 12 additional centers for in-person training by the end of the calendar year.

- Web-based Tool Kit – This tool kit provides 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.[50]

3. Oversight – Fusion Center Privacy Policies

As discussed in last year's annual report, fusion centers are responsible for drafting a written privacy policy that is "at least as comprehensive" as the ISE Privacy Guidelines. The DHS Privacy Office has supported this aim in various ways for years: the Chief Privacy Officer is a co-chair of the Privacy Guidelines Committee (PGC) which promulgated the Guidelines and its section establishing the requirement for non-federal ISE participants like fusion centers. The DHS Privacy Office also led the PGC working group that recommended this standard be communicated to fusion centers through the Global Baseline Capabilities document. The recommendation also appeared in the DHS Privacy Office's 2008 PIA of the Fusion Center Initiative, which the Office sent to every fusion center director across the Nation. The message was also broadcast by the DHS Privacy Office at each of the last two National Fusion Center Conferences in presentations, training, and other material. During the reporting year, the DHS Privacy Office worked to institute two new measures to assure that fusion centers adhere to the privacy principles established in the ISE Privacy Guidelines.

a. Inclusion in DHS Grant Guidance

The Chief Privacy Officer worked with FEMA to ensure that FEMA's FY 2010 Grant Guidance contained the following provision:

> FY 2010 DHS grant funds may not be used to support fusion center-related initiatives unless the fusion center is able to certify that privacy and civil rights/civil liberties (CR/CL) protections are in place that are determined to be at least as comprehensive as the ISE Privacy Guidelines by the ISE Privacy

[50] The tool kit is available at http://www.it.ojp.gov/privacyliberty and is updated regularly to include new guidance and other material relating to the fusion center privacy program.

> Guidelines Committee (PGC) *within 6 months of the award date on this FY 2010 award*. If these protections have not been submitted for review and on file with the ISE PGC, DHS grants funds may only be leveraged to support the development and/or completion of the fusion center's privacy protections requirements.

The DHS Privacy Office is confident that this provision will provide additional incentive to draft and adopt a written privacy policy that meets or exceeds the standards established in the ISE Privacy Guidelines. The Office is similarly convinced that the period of time is sufficient to allow all centers – even those that may have only just begun the process – to develop a meaningful and comprehensive policy.

b. Fusion Center Privacy Policy Review

In November 2009, the DHS Privacy Office, on behalf of the PGC, began an independent review of fusion center privacy policies to determine whether they are "at least as comprehensive" as the ISE Privacy Guidelines.

By the end of the reporting period, the DHS Privacy Office had reviewed and cleared 12 policies, covering 16 fusion centers. In each case, the Chief Privacy Officer issued a letter stating her conclusion that the policy meets the ISE Privacy Guidelines Standards.

This DHS Privacy Office review is typically the last step in a long drafting process. Individual state clearance requirements vary; but in every case, fusion centers take advantage of robust technical assistance offered through the Department of Justice's Bureau of Justice Assistance. Even so, the DHS Privacy Office has commented on a number of policies and withheld approval until changes to the policy were made by the center. Moreover, the Office's review and comments on the first few privacy policies helped inform the PM-ISE's process of revising the templates it developed to assist fusion centers with their drafting.

The DHS Privacy Office anticipates that, given the timetable established under the FY 2010 Grant Guidance, our reviews will become more frequent in the coming reporting period.

4. National Fusion Center Conference

As noted above, the DHS Privacy Office participated in its third straight National Fusion Center Conference. This year's conference was held in New Orleans, Louisiana, on March 22-26, 2010.

The Chief Privacy Officer provided a keynote speech at the conference by addressing the Fusion Center Director's Meeting. While this took place the day before the conference formally opened, it was the best and clearest opportunity to introduce the privacy policy review and the new grant provisions relating to fusion center privacy policies. The Chief Privacy Officer also took the opportunity to renew her recommendation that fusion center directors promote transparency within their centers and eventually undertake a PIA that details: (1) who is in their center, (2) what authorities they are operating under, (3) what systems they access, (4) who they share information with, and (5) what types of products they produce.

The Chief Privacy Officer also participated in a panel discussion during the conference entitled *Privacy 101*. Her presentation focused on the elements of a successful privacy policy including steps to promote transparency, redress, accountability, and data minimization. She introduced attendees to the three-prong training program developed for fusion centers (as discussed above), and urged all fusion center participants to take full advantage of these and other privacy training

opportunities. She concluded her remarks by calling on them to understand their privacy policies, listen to privacy critics, and become privacy advocates in their own centers.

DHS Privacy Office staff conducted a hands-on learning lab during the conference, presenting portions of their *Privacy Fundamentals for Fusion Center Professionals* and answering questions from conference participants. Staff also hosted a booth with CRCL, providing training material, answering questions, and providing advice on all facets of privacy protection practices.

Finally, after the formal close of the conference, the DHS Privacy Office Director of Legislative and Regulatory Analysis and the Acting Deputy for CRCL Programs and Compliance addressed an assembly of all of the I&A intelligence professionals currently assigned to a fusion center, reinforcing the privacy training received in advance of their assignments.

5. Future Plans

The DHS Privacy Office will remain heavily engaged with the fusion center program during the coming reporting year. In addition to the substantial training commitments outlined above, the DHS Privacy Office will support the State and Local Program Office, which provided Department-wide coordination of fusion center support. The Office will also work within the Department to support implementation of the Nationwide Suspicious Activity Reporting Initiative, an important information sharing program with fusion centers and other partners. In support of oversight and compliance, the Office anticipates its review of fusion center privacy policies to increase next year as the deadline established in DHS grant guidance approaches. Finally, during the next reporting year, the DHS Privacy Office will conduct a second PIA of the DHS Fusion Center Initiative.

B. I&A Product Reviews

In April of the reporting period, DHS leadership directed the DHS Privacy Office to begin review of I&A analytical products for privacy related issues before products are released to the intelligence community and our information sharing partners in state and local fusion centers. DHS Privacy Office personnel have reviewed approximately 300 I&A analytical products and 670 Homeland Intelligence Reports.[51] The DHS Privacy Office is confident that its involvement with the review of I&A intelligence products will further strengthen its relationship with I&A and further embed privacy protections throughout the Department and the Department's products.

[51] Homeland Intelligence Reports (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 DHS Privacy Office continued to provide privacy leadership and guidance for the Department's technology initiatives, with a particular focus on cybersecurity, during this reporting year. As always, the Office's goal was to ensure that privacy protections are considered in the development of any new or redesigned DHS system that is privacy sensitive. The Office conducted PIAs, provided training, and worked with other federal agencies to develop privacy policy for government use of new and emerging technologies such as cloud computing. The Office also supported Department efforts to provide greater public transparency into high-profile but classified technology initiatives.

A. Cybersecurity

The DHS Privacy Office and the DHS Office of Cybersecurity & Communications worked closely together to integrate privacy protections into the Department's contributions to the Administration's cybersecurity initiative. Through this work, DHS fostered transparency of the government's cybersecurity activities, implemented privacy compliance procedures, and coordinated with other federal agencies to advance government-wide integrated privacy protections.

1. Privacy Protection and Compliance

DHS has conducted a series of PIAs related to the Department's cybersecurity activities, dating back to 2004 with the first PIA on the EINSTEIN program.[52]

The following PIAs were conducted during the reporting period:

a. Initiative Three Exercise, Classified

DHS conducted a PIA on the Comprehensive National Cybersecurity Initiative (CNCI) Initiative Three Exercise (Exercise), a pilot test of technologies to provide intrusion prevention services to federal executive branch agencies. Aspects of the Exercise are classified and thus exempted from the E-Government Act's requirement to conduct a PIA. Nonetheless, the DHS Privacy Office elected to conduct a PIA on the Exercise at the classified level and made that PIA available to those with appropriate security clearances.

b. Initiative Three Exercise, Unclassified

The classified nature of the Exercise could have presented a barrier to transparency because the classified PIA could not be made publicly available. The DHS Privacy Office, however, produced an unclassified PIA to provide the maximum transparency possible into the classified program. DHS made this unclassified PIA available to the public on the DHS Privacy Office website, thereby providing the most detailed information available about one of the leading

[52] http://www.dhs.gov/xlibrary/assets/privacy/privacy_cybersecurity_white_paper.pdf.

federal government cybersecurity activities.[53] This is the first time the Department has issued an unclassified version of a classified PIA.

c. EINSTEIN 1 Update for Michigan State Proof of Concept

As part of the CNCI, DHS is conducting a proof of concept test with the State of Michigan to determine the benefits and issues presented by deploying the EINSTEIN 1 capability. The DHS Privacy Office requires that pilot programs undergo its privacy compliance process.[54] Therefore, the Office conducted a PIA on the Michigan Proof of Concept to assess the privacy impacts of offering cybersecurity services to the critical infrastructure and key resources sector (including state governments).

2. Privacy in Cybersecurity Training

The DHS Privacy Office developed online privacy training that DHS cybersecurity staff uses to understand the privacy risks associated with IT systems and steps that can be taken to mitigate those risks. The training course addresses ways in which systems may affect privacy and explains the privacy documentation required to use them.

3. Transparency and Outreach

DHS has provided transparency into its cybersecurity activities through engagement with the DPIAC and through direct communication with the public. See Part Two, Section IV for further discussion of DPIAC activities during the reporting period.

a. Data Privacy & Integrity Advisory Committee

The Chief Privacy Officer requested guidance from the DPIAC on privacy issues related to the Department's cybersecurity activities. In response, a subcommittee was created to focus specifically on DHS's cybersecurity programs and systems and to report its findings to the DPIAC. The DPIAC Cybersecurity Subcommittee includes several DPIAC members, as well as other subject matter experts including privacy advocates, representatives of academia, and the civil liberties community. A portion of the Department's cybersecurity efforts are classified, and Subcommittee members have security clearances appropriate for those efforts.

To date, DHS has provided a series of classified briefings to the DPIAC Cybersecurity Subcommittee, including briefings on the CNCI, on specific cyber threats facing the federal government, and on the Department's responsive actions. DHS will continue these classified briefings and seek DPIAC guidance as the Department continues to advance the defense of computer networks against cyber threats.

b. Privacy & Cybersecurity Website

DHS continues to build upon each discrete transparency effort with a new section of the DHS privacy website specifically devoted to the integration of privacy protections into DHS

[53] The unclassified PIA for the Initiative Three Exercise is available on the DHS privacy website: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf.
[54] The DHS Privacy Office formalized the inclusion of pilot tests in the scope of its privacy compliance review in its Privacy Policy Guidance Memorandum 2008-02, available on the DHS privacy website: http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-02.pdf.

cybersecurity activities.[55] This new section, which is available directly from the DHS Privacy Office homepage, provides links to relevant PIAs and cybersecurity-related testimony before the DPIAC, and provides an index to the White House's cybersecurity information, including the declassified description of the CNCI. As DHS continues to develop cybersecurity programs and systems, the Department will update this website to provide a current index to those cybersecurity activities and their embedded privacy protections.

c. White Paper on Security and Privacy Protections in DHS computer networks

On February 19, 2010, the DHS Privacy Office and the DHS Office of Cybersecurity and Communications published a white paper entitled *Computer Networking Security and Privacy Protection* describing the Department's cybersecurity activities and the way DHS integrates privacy protections into cybersecurity planning and operations.[56] The white paper preceded the White House's declassified description of the CNCI. It discusses the background and authorities for DHS cybersecurity activities; specific descriptions of DHS cybersecurity activities, including sections dedicated to the Trusted Internet Connection and the Einstein Two Initiative (including how EINSTEIN collects information using signatures); individual agency responsibilities as they participate in the EINSTEIN program; and the roles of the National Security Agency and the private sector.

4. Interagency Coordination

The Department's cybersecurity activities are part of a larger federal government effort to improve cybersecurity for the nation and internationally. In order to ensure privacy considerations are addressed consistently throughout the federal government and to share privacy insights into cybersecurity activities, DHS coordinates with other federal agencies through the White House-led Civil Liberties, Privacy Rights and Authorities sub-IPC of the Information and Communications Infrastructure Interagency Policy Council (IPC). During this reporting period, the DHS Privacy Office attended several meetings of this group to discuss cybersecurity efforts across the federal government (both classified and unclassified). The DHS Privacy Office provided advance copies of the classified PIA for the Initiative Three Exercise to this Interagency Group to coordinate the various equities engaged in the Exercise and to provide intragovernmental transparency to the privacy officers of other federal agencies. See Part One, Section VII.C.3 for additional information on DHS Privacy Office participation in IPC activities.

B. 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.[57] The

[55] The specific URL for the privacy and cybersecurity webpage is: http://www.dhs.gov/files/publications/editorial_0514.shtm#4.

[56] The white paper is available on the DHS Privacy Office website: http://www.dhs.gov/xlibrary/assets/privacy/privacy_cybersecurity_white_paper.pdf.

[57] 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. http://www.whitehouse.gov/blog/Streaming-at-100-In-the-Cloud/.

DHS Privacy Office has been actively involved in this initiative from the beginning. During the reporting period, the DHS Privacy Office participated on the Federal CIO Council Privacy Committee's Web 2.0 Subcommittee to identify privacy risks associated with cloud computing and to define best practices for federal agencies. See Part One, Section VII.C.1 for further description of the DHS Privacy Office's work on the Federal CIO Council Privacy Committee.

The DHS Privacy Office was also involved in the Federal CIO Council's Cloud Computing Security and Standards Working Groups. These groups are multi-agency efforts including representatives from the National Aeronautics and Space Administration, Department of Defense, SSA, Department of Energy, and General Services Administration. The DHS Privacy Office has been working with the Federal CIO Council's process known as FedRAMP (Federal Risk and Authorization Management Program) to ensure privacy is considered throughout the planning and implementation stages of cloud computing.

VI. Policy Initiatives

The Office is always at the forefront of DHS privacy policy, and this reporting year was no exception. The Office was intensively involved in the development of Department policy for information sharing both within DHS and with external partners, to build privacy protections into information sharing agreements. Together with the DHS CISO, the Office issued a new policy on privacy protections for machine-readable extracts of sensitive PII taken from Department systems. The Office also published a guide describing its operations, to both educate DHS employees and provide the public greater transparency into how privacy policy is developed and implemented at DHS. All of these efforts served to further the culture of privacy at DHS.

A. Information Sharing

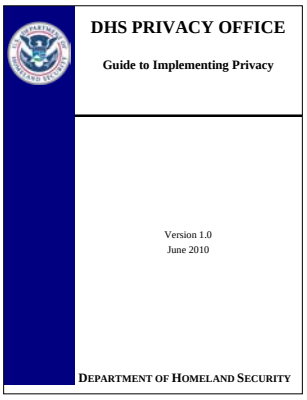
As DHS has continued to refine its processes for information sharing within the Department and with federal, state, local, territorial, and tribal partners, the DHS Privacy Office has remained active in building privacy protections into those processes. The Chief Privacy Officer is an *ex officio* member of the DHS Information Sharing Governance Board (ISGB), a body consisting of senior leaders from each of the DHS components. The ISGB is the senior steering committee and policy-making body for information sharing practices at DHS. Senior members of the DHS Privacy Office also serve as action officers for the Information Sharing Coordination Council (ISCC), which supports the ISGB and develops policy recommendations and guidance.

The ISCC has recently promulgated two significant advances in DHS information sharing policy and practices. First, the ISCC established the Data Access Review process (DAR). The DAR is a formalized process for reviewing requests for DHS information from external DHS partners. It requires the DHS Privacy Office, OGC, CRCL, and the DHS component responsible for the data to review and approve requests for access to DHS data at the earliest point in the development of an information exchange. The ISCC also issued a revised *Information Sharing Access Agreement Guidebook and Templates*, a comprehensive guide to developing DHS Information Sharing Agreements. Members of the DHS Privacy Office took the lead in developing revisions to the Guidebook on privacy considerations and model language for information sharing agreements. This work was based in part on the DPIAC's May 2009 recommendations.[58]

The ISCC also reviews all DHS Information Sharing Access Agreements before the agreements become final. As action officers of the ISCC, senior members of the DHS Privacy Office participate in those reviews to ensure the agreements comply with DHS privacy policies, including ISCC guidance, and provide feedback and guidance on incorporating privacy protections into information sharing agreements.

[58] *A White Paper: DHS Information Sharing and Access Agreements, Report No. 2009-01* (May 14, 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_issa_final_recs_may2009.pdf.

B. Privacy Guide



In last year's Annual Report, the DHS Privacy Office discussed ongoing work on a handbook describing how the Office implements privacy throughout the Department. In June 2010, the Office published the handbook, now entitled the *DHS Guide to Implementing Privacy*.

The Guide is a comprehensive resource for in-depth information regarding DHS Privacy Office functions. The purpose of the Guide is to inform the Department, other federal agencies, and the public about the DHS Privacy Office and provide transparency into its various functions and operations. The Guide will also aid in orienting new DHS Privacy Office personnel, new component privacy officers and PPOCs, other federal privacy officers, and international partners by providing insight into how DHS builds its privacy culture.

The Guide discusses the DHS Privacy Office's role and responsibilities as steward for privacy within the Department. It covers policy development, compliance, education and awareness, complaints and incident reporting, public outreach and transparency, international activities, disclosure and FOIA operations, and reporting. The Guide summarizes, but does not replace, existing DHS Privacy Office policies, procedures, and guidance. It is available on the DHS Privacy Office website.[59]

C. Computer-Readable Extracts Policy

The DHS Privacy Office completed the *DHS Policy and Procedures for Managing Computer-Readable Extracts (CREs) Containing Sensitive PII* (CRE Policy) during the reporting period. In July 2008, the Office established a Data Extracts Working Group to respond to OMB requirements outlined in OMB Memorandum 07-16 requiring federal agencies to log and track data extracts of sensitive information from systems in computer-readable formats. This Working Group developed the CRE Policy, which provides baseline standards to minimize the risks associated with CREs and outlines uniform practices at DHS for authorizing, tracking, and destroying CREs. The Working Group focused on non-routine or ad hoc data extracts and methodologies for reducing the likelihood of losing sensitive information while limiting the impact to DHS business operations. The DHS Privacy Office is currently working with the DHS CISO to promulgate the CRE Policy, together with a set of frequently asked questions (FAQs) and training slides to educate DHS staff on the CRE Policy requirements. The Office's work with the CISO's Office in drafting and publishing the CRE policy has been critical to ensuring a coordinated and seamless implementation of the CRE Policy across DHS. The CRE Policy requirements are included in Section 3.14.5 *Protecting Privacy Sensitive Systems* of the *DHS Sensitive Systems Security Policy 4300A* and the policy and procedures will be added to an upcoming version of 4300A Handbook, as Appendix S1.

[59] http://www.dhs.gov/xlibrary/assets/privacy/privacy_implementation_guide_june2010.pdf.

D. Homeland Security Grants for CCTV

In 2007, the DHS Privacy Office and CRCL issued a report entitled *CCTV: Developing Privacy Best Practice, Report on the DHS Privacy Office Public Workshop* (CCTV Report), which provides resources for implementing privacy safeguards in closed circuit television (CCTV) systems, including a set of best practices for government use of CCTV and a PIA for state and local entities to use in assessing the privacy impacts of their deployment of CCTV.[60] During the current reporting year, the DHS Privacy Office collaborated with FEMA to include a new provision in the FY 2010 FEMA Grant Guidance on government grantees applying for funding for CCTV-related operations. The provision recommends that grantees seeking funds to purchase or install CCTV, or to provide support for CCTV systems that are already operational, review and utilize the guidance provided in the CCTV Report. The new provision is a significant step toward ensuring that FEMA grantees implement CCTV systems in a manner that both furthers their security missions and respects privacy.

[60] The CCTV Report is discussed more fully in the DHS Privacy Office's 2009 Annual Report (http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf) and is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_cctv_2007.pdf.

VII. Collaboration Within and Outside DHS

The DHS Privacy Office engages with many individuals, groups, and agencies both inside and outside of the Department. These relationships help support the DHS Privacy Office in achieving its mission to educate others about the Office's activities and responsibilities, advocate best practices, and contribute to the broader privacy community. Internal DHS offices, federal agencies, and international partners all play an important role in the collaboration efforts of the Department. Several of these efforts are discussed in the following sections.

A. Office for Civil Rights and Civil Liberties

Section 222(a)(5)(A) of the Homeland Security Act requires the Chief Privacy Officer to "coordinat[e] with the Officer for [CRCL] to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner."[61] The DHS Privacy Office and CRCL continued to work closely during the reporting year on a wide variety of DHS programs including, but not limited to, information sharing access agreements with external DHS partners, intelligence product review, a DHS-wide SORN, human resources matters, and a number of other programs. The two offices held bi-weekly teleconferences to discuss issues of common concern. The two offices also worked closely together in support of the DHS State and Local Fusion Center Program. For the third straight year, the DHS Privacy Office and CRCL co-hosted a booth at the 2010 National Fusion Center Conference in New Orleans, Louisiana. The two offices also continued their close collaboration to develop and deliver training to state and local fusion centers across the U.S. This training is discussed in further detail in Part One, Section IV.A.2 of this report.

Together with CBP Privacy staff, the DHS Privacy Office and CRCL also reviewed and assessed the training CBP officers receive regarding searches of electronic devices at U.S. borders. All three offices undertook an independent initial review and joint follow up review to discuss observations and recommendations. A public report on their findings was issued shortly before this annual report was released.[62]

B. Office of the Chief Information Security Officer

Throughout the year, the DHS Privacy Office coordinated with CISO on a number of projects. The DHS Privacy Office participated in weekly DHS CIO Council meetings and in meetings of the CISO Council Security Policy Working Group. During these meetings, the Office provided

[61] 6 U.S.C. § 142(a)(5).
[62] The report, entitled "*U.S. Customs and Border Protection Border Search of Electronic Devices Containing Information Training: Assessment and Recommendations"* (August 20, 2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-report-cbp-training-border-searches-electronic-devices.pdf.

updates regarding privacy training initiatives and projects that may require the participation of, or be of interest to, the DHS CIO, the DHS CISO, and/or the component CISOs. The DHS Privacy Office was also able to gain a better understanding of systems being considered for development, planned and proposed changes to existing systems, systems being retired, information changes, and updates to information security policies and procedures that could impact privacy (e.g., updates and changes to version 7.2.1 DHS Directive 4300A and DHS 4300A Handbook). Participation in these meetings ensures that privacy and security are addressed in unison and promotes efficiency and coordination among the CIO, the CISO, and the DHS Privacy Office. In addition to attending CIO and CISO meetings, the DHS Privacy Office reviewed and provided substantive comments to CISO on documents that impact privacy, including the CISO's Social Media guidance, and the Information System Security Officer (ISSO) Guide. See Part One, Section II.D for additional discussion on the Compliance Group's work with the CIO and CISO.

C. Collaboration within the Federal Government

1. Federal Chief Information Officers Council, Privacy Committee

The Chief Privacy Officer serves as co-chair of the Federal CIO Council[63] Privacy Committee, the organization of federal senior agency officials for privacy and chief privacy officers established in 2008 to serve as the principal interagency forum for informing policy development and improving practices for protecting privacy across the federal government. In addition to the Chief Privacy Officer's role, senior members of the DHS Privacy Office staff serve as co-chairs of the Privacy Committee's Best Practices and International Subcommittees.

The Privacy Committee has been involved in several important initiatives during the reporting period. The Privacy Committee hosted a Chief Privacy Officer Boot Camp, a forum designed specifically for incoming chief privacy officers across the federal government. Incoming chief privacy officers heard presentations on a variety of topics ranging from how to implement an agency-wide privacy program to privacy incident response. The Privacy Committee also hosted a Privacy Summit for all federal privacy professionals. Privacy professionals attended training sessions and heard speakers discuss topics salient to privacy practices in the federal government.

The Privacy Committee contributed to the review of the OMB M-03-22 Cookie Policy[64] via the Web 2.0 Subcommittee. The Privacy Committee's Identity Management Subcommittee has contributed to several working groups focused on identity, credentialing, and access management, and has developed a model PIA for federal agencies using federated identity credentials.

The DHS Privacy Office co-chairs the Privacy Committee's Best Practices Subcommittee with the Federal Deposit Insurance Corporation and the Department of Energy. During the reporting period, the Subcommittee continued its work on several projects intended to further privacy protections throughout the federal government. The Subcommittee provided guidance on privacy best practices for OMB's Federal Enterprise Architecture and finalized a white paper for

[63] 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.
[64] OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*: Section III, September 26, 2003.

federal agencies on how to establish an effective, comprehensive federal agency privacy program. The white paper, entitled *Elements of a Federal Privacy Program*, was published by the Privacy Committee in June 2010.[65]

The DHS Privacy Office also co-chairs the International Subcommittee with the Department of State. The Subcommittee worked on several initiatives in the past year, including cataloguing privacy provisions of international agreements, collecting information on foreign privacy standards and laws, developing a standard international briefing on the U.S. privacy framework, and reviewing U.S. government agencies' "mixed systems" policies. See Part One, Section VII.C.1 for additional discussion on privacy initiatives undertaken by the Federal CIO Council's Privacy Committee.

2. Federal Chief Information Officers Council, Identity, Credential, and Access Management Committee (ICAM)

The DHS Privacy Office expanded its participation in the Federal CIO Council by joining ICAM, which is responsible for developing the Federal Identity, Credential, and Access Management (FICAM) "Roadmap and Implementation Guidance" (FICAM Roadmap). The FICAM Roadmap is the comprehensive guide for implementing online identity assurance services for federal government websites. Senior members of the DHS Privacy Office staff provided subject matter expertise for the FICAM Roadmap's guidance on incorporating privacy in the implementation of online identity assurance solutions. Members of the DHS Privacy Office also participated in developing the criteria to evaluate applications from organizations seeking to provide online identity assurance services to federal government agencies through the Trust Framework Provider Adoption Process, and served on the evaluation team for those applications (called the Trust Framework Evaluation Team or TFET).

3. Interagency Policy Council

The DHS Privacy Office also participates in the Interagency Policy Council's Subcommittee on Architecture, Research, and Development (ARD sub-IPC). Recently the ARD sub-IPC has focused on development of the draft National Strategy for Trusted Identities in Cyberspace (NSTIC), which was issued for public comment on June 25, 2010. NSTIC is an initiative, undertaken in response to the National Security Staff's 2009 Cyberspace Policy Review, to develop and strengthen identity authentication solutions for online transactions across all sectors. While identity management solutions have been evolving in both the public and private sector, the Cyberspace Policy Review pointed to a need for a comprehensive national strategy to build trust for online transactions and to enhance privacy. Senior members of the DHS Privacy Office are on the writing team for NSTIC, and have successfully advocated for the use of the FIPPs as the baseline for integrating privacy protections in online identity authentication. NSTIC is scheduled to be formally released in fall 2010.

[65] The white paper is available on the CIO Council's website at http://www.cio.gov/documents_details.cfm/uid/8A528FDC-5056-8F64-369CC7FF6FEDB72D/structure/Information%20Technology/category/Best%20Practices.

VIII. Training & Education

The DHS Privacy Office partners with other offices in the Department to develop mandatory privacy training for all employees and contractors, and to include privacy themes in supplemental training classes. The Office reports quarterly to Congress on its training activities as required by Section 803 of the 9/11 Commission Act. The Office also supports targeted training efforts, such as compliance training and specific role-based courses within the Department. These training courses are discussed in the subsections that follow. The DHS Privacy Office also supports privacy training for state and local fusion centers, as discussed in Part One, Section IV.A.2, and for DHS cybersecurity staff as discussed in Part One, Section V.A.2.

A. DHS-wide Education and Training

The DHS Privacy Office continued to execute its ongoing responsibility to ensure that DHS employees understand the privacy implications of their daily work, and handle PII responsibly and in accordance with the Privacy Act and DHS Privacy Office guidance. To that end, the Office provided both mandatory and supplemental privacy training for DHS employees in a number of different formats and venues.

1. Mandatory Training

The Privacy Act[66] and OMB Circular A-130[67] mandate annual Privacy Act training for DHS employees and contractors. The DHS Privacy Office provides introductory privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees. A new 30-minute course was introduced in April 2010.

This initial privacy training is supplemented by the DHS Privacy Office's *A Culture of Privacy Awareness* computer-based course, which covers the essentials of the Privacy Act and the E-Government Act, as well as the responsibility of DHS employees to use PII only for authorized purposes and to protect it from misuse or loss. *A Culture of Privacy Awareness* is mandatory for all DHS employees and is available to DHS headquarters employees through DHScovery, the Department's web-based learning management system. The DHS Privacy 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 are implementing 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 IX of this report. Currently the office is preparing an updated and improved version of *A Culture of Privacy Awareness.*

[66] 5 U.S.C. 552a(e)(9).

[67] 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.

The DHS Privacy Office provides a privacy presentation during the two-day *DHS 101* training course, which takes place monthly and is now required for all new and existing headquarters staff. *DHS 101* provides an overview of all DHS components' roles and activities. The content for this course was also revised and relaunched in March 2010.

With the hiring of an Associate Director of Communications and Training in November 2009, the DHS Privacy Office is aiming to systematize privacy training across the Department during the next reporting year.

2. Supplemental Training

Increasingly, the Department's overseas partners and allies have engaged in discussions about the U.S. privacy framework. To improve the chances for success of planned DHS aviation security and other information sharing initiatives, the DHS Privacy Office undertook a training initiative to formally advise new DHS outbound attachés and liaisons stationed abroad of the policy implications that misunderstandings of U.S. privacy laws and DHS privacy policies may have on international cooperative activities. Strengthening attachés' and liaisons' understanding of these issues before deployment will help them to identify privacy concerns that may impact DHS activities, improve the dialogue with international partners, and help dispel misperceptions. While every DHS employee is required to undergo annual privacy training, this proposed training will be customized to the needs of DHS employees posted abroad, with a focus on privacy policy. This program will be formalized during the next reporting period to include remote learning opportunities. See Part Three, Section IV for additional information on the outbound attachés and liaisons training initiative.

3. Compliance Training

During this reporting year, the Compliance Group redesigned its annual compliance training workshop for DHS employees and contractors. This year's workshop, held in June 2010, centered around the theme of piecing privacy together and putting it into context with other Departmental processes including: information security and FISMA, the systems development lifecycle, Departmental rules and regulations, and the PRA. The workshop, entitled *Pieces of Privacy* covered a brief history of U.S. privacy as well as the full suite of privacy compliance documentation including PTAs, PIAs, SORNs, Privacy Act exemptions, and Privacy Act e(3) statements required when collecting PII on forms. The new PTA, PIA, and SORN templates were also released during the training. To reinforce the theme of how privacy fits into other missions and functions of the Department, the workshop featured speakers from offices within and outside the Department. The training was well attended by both DHS and other federal agencies.

B. Role-Based Education and Training

1. DHS Privacy Office Staff Training

In addition to training others, DHS Privacy Office staff participated in national conferences and specialized training programs throughout the year to stay current on recent developments in privacy law and policy. DHS Privacy Office staff regularly attended conferences of the International Association of Privacy Professionals (IAPP) and the American Society of Access Professionals (ASAP), the professional organization for federal government employees and private citizens working in the field of access to information under FOIA and the Privacy Act. The DHS Privacy Office staff also participated in IAPP credentialing programs, as discussed in Part One, Section VIII.E.

2. Intelligence and Analysis Training

Section 511 of the 9/11 Commission Act[68] requires that DHS I&A employees assigned to state and local fusion centers undergo appropriate privacy training developed, supported, or sponsored by the DHS Privacy Office. The DHS Privacy Office continued to train intelligence analysts assigned to fusion centers during the reporting period. Fusion center training is discussed more fully in Part One, Section IV.2.

C. DHS Speaker Series

The DHS Privacy Office is in its third year of hosting the DHS Privacy Office Speaker Series. The Speaker Series provides the Office an opportunity to host outside experts for informal discussions with DHS staff on privacy-related topics.

In March 2010, the DHS Privacy Office hosted a well attended event during which Daniel J. Weitzner, Associate Administrator for the Office of Policy Analysis and Development in the National Telecommunications and Information Administration, U.S. Department of Commerce, spoke on Internet Policy 3.0, the nexus between privacy and innovation. Mr. Weitzner discussed the challenges of developing and implementing policies in an expanding and dynamically changing information ecology. Mr. Weitzner also spoke about his prior work at MIT on disruptive technologies and the related policy challenges.

D. Component Privacy Events

The DHS Privacy Office fosters a culture of privacy throughout the Department by encouraging DHS components to sponsor events to raise privacy awareness among their staff. Several components began hosting annual privacy events in FY 2010. These events, which met with much success, are described in the following sections. As a way to demonstrate synergies and the interconnected relationship of the DHS Privacy Office and the components, the Chief Privacy Officer spoke during every component privacy event.

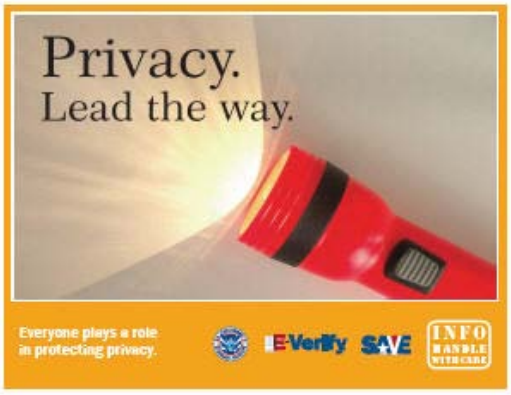
[68] 6 U.S.C. § 124h(c)(4)(A).

1. US-VISIT

In October 2009, the U.S. Visitor and Immigrant Status Indicator Technology Program (US-VISIT) held its second Annual Privacy Awareness Week, which provided the opportunity for all US-VISIT employees and contractors to recommit to protecting personal information. Federal privacy subject matter experts conducted presentations on identity theft, privacy, and social engineering and provided real-life examples and recommendations on how to prevent privacy and security breaches. Privacy and data protection posters were displayed throughout US-VISIT's office spaces and remain on display to remind staff of the importance of privacy and data protection at US-VISIT. Over 200 US-VISIT employees, contractors, and DHS Privacy employees attended Privacy Awareness Week events.

2. USCIS Verification Division

In conjunction with the U.S. Citizenship and Immigration Services (USCIS) Privacy Office, the Privacy Branch of the Verification Division held its second annual Privacy Awareness Month in May 2010. Speakers throughout the month included the Chief Privacy Officer; the Executive Director, Privacy and Acting Chief Information Officer, Office of Information Security, Social Security Administration; and the Director, Privacy Information Protection, Internal Revenue Service.



A key component of Privacy Awareness Month included role-based privacy training that targeted the unique training needs of each division branch including the four field offices. Fifteen different training sessions were held for field office and headquarters staff totalling over 300 participants. During the month, weekly privacy tips were also distributed to Verification Division personnel via the Verification weekly newsletter to raise awareness of privacy issues, challenges, and regulations. Topics included "Is Your Password Buff," which provided information on how to create a strong password; "This Time it's Personal," which provided tips on how to clean up personal papers; "Keep it Green," which reminded staff to reduce the amount of printing, and "Clean up your electronic files; it's as easy as 1,2,3, DELETE." A poster campaign, flyers, and trivia contests designed to further promote privacy principles among Verification Division personnel were also incorporated into the program.

3. Science & Technology

In April, S&T held its third annual privacy awareness training event, Privacy Week 2010, during which the Chief Privacy Officer spoke on the importance of privacy awareness and on the work of the DHS Privacy Office. During Privacy Week, S&T accomplished the following objectives:

- Conducted Directorate-wide mandatory annual privacy awareness training for all S&T employees and contractors, including personnel at S&T offsite laboratories and S&T Federally-Funded Research and Development Centers.
- Provided supplemental training for Program Managers that focused on the new S&T Privacy SharePoint site. S&T will implement new workflows and document

management through SharePoint, as well as better integrate the compliance process into SharePoint.

- Audited mobile devices to ensure compliance with DHS policies and regulations regarding the storage and retention of PII.
- Conducted a "file clean up," during which S&T personnel reviewed paper and electronic files to identify PII, delete or dispose of files that are no longer needed, and properly protect files that must be retained.
- Coordinated a Q&A session in which several S&T Program Managers met with DHS Privacy Office staff to discuss privacy concerns and questions related to specific S&T projects.
- Coordinated with CRCL to provide a training session for S&T Program Managers and Division Directors on how CRCL can assist S&T in identifying and addressing civil rights and civil liberties issues in S&T research projects.

E. Certification

During this year, the DHS Privacy Office continued to develop the expertise of its privacy and FOIA professionals by encouraging participation in certification programs and training courses to enhance their skills and abilities while furthering the mission of the Office and the Department. Several DHS Privacy Office staff members were successful in obtaining the IAPP Certified Information Privacy Professional/Government (CIPP/G) certification. This certification is the first publicly-available privacy certification designed for federal government employees with privacy-related responsibilities or obligations, such as privacy officers, compliance managers, records managers, access-to-information coordinators, information security managers, and information auditors. To be recognized as a CIPP/G, privacy professionals must pass both the IAPP's Certification Foundation and CIPP/G examinations. At the conclusion of the reporting year, 21 staff in the DHS Privacy Office held the CIPP/G certification and four held the CIPP certification. The DHS Privacy Office encourages privacy staff throughout DHS to obtain this certification.

IX. Highlights of Component Privacy Programs and Initiatives

Component privacy programs 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 programs have grown significantly. As noted previously, in response to the Deputy Secretary's June 2009 instruction several privacy officers have been added or their authorities increased over the past year. See Part One, Section I. This section highlights some of the key privacy-related activities undertaken by CBP, FEMA, I&A, ICE, S&T, TSA, USCG, USCIS, USSS, and US-VISIT/NPPD during the reporting period.

A. CBP

CBP's unique role at the border provides it with access to a broad array of data concerning persons and commodities crossing the U.S. border. This information serves a variety of border security, trade compliance, and law enforcement purposes for federal and state governments. CBP's focus for this reporting period has been on the sharing of import information to allow for the identification and seizure of unsafe imports. In addition to cross-component collaboration activities and drafting PIAs and SORNs, CBP devoted significant resources during the reporting period to provide operational support and transactional privacy compliance to the federal and state law enforcement mission. In order to receive authorization to share information, the use of the information must be compatible with the purpose for collecting the information as documented in a PIA and SORN. Each request for authorization covers a specific information sharing transaction with a federal, state, local, tribal, or foreign agency. CBP prepared over 450 such authorizations during the reporting period, in addition to those instances of sharing covered by a memorandum of understanding.

1. Border Searches of Electronic Devices

As discussed in the 2009 Annual Report and above in Part One, Section II.B.2 of this report, DHS's Chief Privacy Officer directed CBP and ICE to conduct a FIPPs-based PIA evaluating the privacy concerns and policies related to the search and seizure of electronic devices and the information contained within them. DHS published this PIA on August 27, 2009. Due to the sensitive information that individuals can store on their laptops and other electronic devices, CBP and ICE used this opportunity to review this important, yet sparingly used, law enforcement tool to bring increased transparency to the public.

The PIA provides a detailed discussion of the Department's, CBP's, and ICE's exercise of discretion in implementing their substantial border search authority. The PIA also provides copies of the ICE and CBP directives that establish, respectively, agency policy and practice in the exercise of the border search authority. These directives establish firm timeframes for returning detained electronic devices and clear procedures for handling sensitive information.

Further, tearsheets and new signs were first disclosed in the PIA and then, at most 30 days later, distributed at ports of entry to better inform those individuals whose devices may be searched.

Specifically within the PIA, CBP and ICE present DHS's general border security mission, definitions of commonly used terms, and the parameters for both CBP and ICE to conduct a border search of an electronic device. Additionally, the PIA sets forth the procedural requirements for memorializing the factual details of the border search process concentrating on: why CBP and ICE conduct searches; how CBP and ICE handle electronic devices and the information that is stored on them; and the policies and procedures in place to protect individuals' privacy. This PIA concludes with a privacy risk and mitigation analysis of those policies and procedures based on the FIPPs. Further details on the PIA are provided in Part One, Section II.B.2 of this report.

The following discussion provides a snapshot of how the border search authority is employed with respect to electronic devices. For the reporting period October 1, 2009 to April 30, 2010, CBP encountered more than 168.2 million travelers at U.S. ports of entry. Of these travelers, approximately 3.7 million (2.2% of the 168.2 million travelers) were referred for secondary inspection; however, of these 3.7 million travelers, CBP conducted only 2,272 searches of electronic media during this time period. A "search" in this regard is broadly defined to include a simple request to turn the device on as a means of ensuring that it is what it purports to be. Detailed information on these searches is only available for those performed on laptops. Of the total number of searches of electronic media, only 673 searches of any type were performed on laptops – just 0.0184% of the 3.7 million travelers referred to secondary inspection.

2. Commercial Targeting and Analysis Center

CBP established a commercial targeting center in October 2009 as a mechanism for agencies to share targeting resources, analyses and expertise, and to achieve the common mission of protecting U.S. citizens from unsafe imports. CBP and the U.S. Consumer Product Safety Commission (CPSC) signed a memorandum of agreement that provides CPSC personnel access to import data in CBP's Import Safety Commercial Targeting and Analysis Center. Through the Center, CPSC conducts import safety risk assessments and performs targeting work using CBP's Automated Commercial System and Automated Commercial Environment. Import data analyzed and shared through the Center includes names, addresses, and other contact information for importers, exporters, shippers, carriers, brokers, and other persons involved in a transaction. Shared PII may also include an importer's Tax Identification Number. CBP anticipates that it will sign similar agreements with both the Food and Drug Administration and the U.S. Department of Agriculture's Food Safety Inspection Service.

3. Information Sharing

CBP has diligently worked to enhance its information sharing to support privacy generally and privacy compliance in all instruments that execute information sharing at the international, federal, state, and local governmental levels. CBP has created a work process wherein one-time information requests as well as requests for recurring information sharing are drafted and reviewed by the CBP Privacy Office.

Concerning one-time information requests from local, state, and federal agencies and other international government agencies, requests received in the field are sent to a central location – CBP Privacy mailbox – for review by one of the four privacy attorneys assigned to CBP

Privacy's information sharing practice group. Upon review, the responding privacy attorney drafts an authorization memorandum instructing the field personnel whether or not the requested information can be released to the local, state, or federal agencies, or other international requestors. If the determination is that the requested sharing is consistent with applicable privacy policies, the memorandum instructs the field personnel about the process in place for release of the requested information and about any redactions that may be necessary prior to release to the requestor. The memorandum also explains any limitations on the use of the information that must be explained in the cover letter accompanying the shared record(s). In the last year, the CBP privacy office reviewed approximately 450 requests, issuing an individual authorization memorandum in each case.

CBP has also worked to ensure privacy principles are applied in memoranda of agreement with other agencies concerning requests for recurring information sharing. The main focus this year has been on the sharing of import information including PII of importers, exporters, shippers, carriers, brokers, and other persons involved in a transaction, to allow for the identification and seizure of unsafe imports.

4. Participation in International Privacy Groups

In February 2010, the CBP Privacy Office, led by the information sharing team lead, represented CBP at the inaugural meeting of the World Customs Organization's (WCO) United Nations Commission on International Trade Law Joint Legal Task Force on Coordinated Border Management Incorporating the International Single Window working group.[69] Topics identified in the meeting for initial analysis included mutual recognition of identification and authentication procedures, electronic documents and messages, requirements for admissibility of e-evidence, identification, authentication, and authorization and information sharing among various government entities. The WCO Secretariat agreed to gather "real world" Single Window examples as well as hypothetical models for review and to issue formal written requests to the respective customs agencies for assistance with these matters.

5. Support for International Reviews

As part of the DHS Privacy Office-led delegation participating in the 2010 European Union (EU)-U.S. Passenger Name Record (PNR) Agreement Review, the CBP Privacy Office provided support in drafting updates to both internal field guidance for CBP Officers and external public notifications. Prior to the commencement of the Review in February 2010, CBP posted updates to its PNR Privacy Policy and to its PNR FAQs. During the Review, the CBP Privacy Officer responded to redress and access concerns raised by the EU delegation, and provided supporting information with respect to CBP's information handling practices in compliance with the terms of the 2007 EU-U.S. PNR Agreement. For a discussion of the DHS Privacy Office's International Privacy Policy Group's work in connection with the PNR Review, see Part Three, Section II.D of this report.

[69] A single window system enables traders to submit regulatory documents required by a variety of different agencies at a single location or single entity. Such documents are typically customs declarations, applications for import or export permits, and other supporting documents such as certificates of origin and trading invoices. In a traditional pre-Single Window environment, traders may have had to interact with multiple government agencies in multiple locations in order to obtain the necessary papers, permits and clearance to complete their import or export processes.

B. FEMA

FEMA's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

Since July 2009, FEMA has undertaken a series of initiatives designed to improve privacy compliance, risk management, and privacy awareness throughout Agency operations.

1. Resources

On February 15, 2010, FEMA appointed as its Privacy Officer a Senior Executive Service-level official devoted exclusively to privacy, a first for the Agency. In addition, FEMA added three permanent, full-time employees to its privacy staff. The new privacy staff will support the FEMA Privacy Office's core functions of compliance, incident response, mitigation, and training. The new FEMA privacy team will also strengthen FEMA's existing efforts to increase privacy awareness and compliance and to systematize a culture of privacy throughout the Agency.

2. Compliance

Due to the effect of natural disasters directly upon individuals, FEMA routinely collects PII from applications submitted by survivors seeking assistance and by applicants requesting assistance to help prevent and prepare for flood-related disasters. FEMA collaborates with the DHS Privacy Office to ensure that its systems and programs are compliant with all requirements of the Privacy Act, E-Government Act, DHS policy, and other privacy mandates. Through privacy compliance processes, particularly the PTA and the PIA, FEMA identifies opportunities to reduce its holdings of PII. In addition, the compliance process serves as a mechanism to improve public awareness of FEMA's information collection practices.

In addition to completing PTAs, PIAs, and SORNS, FEMA collaborated with the U.S. Small Business Administration on a CMA. FEMA also established a plan to develop programmatic overarching PIAs, which cover multiple systems having a similar purpose. The Grant Management Programs PIA was published on July 14, 2009; the Training and Exercise Programs PIA is in development and slated for publication by this fall. Developing PIAs that cover more than one system improves efficiency and consistency within the privacy compliance process by eliminating the duplicative process of completing individual PIAs for similar systems and assuring that similar systems safeguard PII consistently.

3. Privacy Incidents and Complaints

FEMA responds to privacy incidents according to its established PII incident standard operating procedures to ensure timely response, coordination, and mitigation of privacy incidents, thus lowering the risk of potential harm to affected individuals. The FEMA Privacy Office has developed a tracking mechanism to identify trends that may exist among privacy incidents. The FEMA Privacy Office also provides remediation recommendations, which have led to a decrease in recurrence of similar incidents. The FEMA Privacy Office did not receive any privacy-related complaints during this reporting period. To further safeguard PII and reduce its risk of privacy

incidents, FEMA is issuing encrypted, password-protected portable "thumb drives" to employees.

4. Training and Related Activities

FEMA is committed to increasing privacy awareness throughout the Agency by expanding the availability of privacy training, including providing instructor-led training, to FEMA staff throughout FEMA's 10 regions across the country. The FEMA Privacy Office undertook the following initiatives during the reporting period:

- Incorporated privacy awareness training into the Enter-On-Duty Orientation for new employees. This effort, in conjunction with FEMA's ongoing presentation of privacy awareness training during its New Contractor Orientation, allows FEMA to raise the visibility of its new Privacy Office, impress upon new National Capital Region staff the importance of safeguarding PII, and increase privacy awareness within the Agency. The privacy awareness training includes such topics as defining PII, employee obligations under the Privacy Act, and reporting privacy incidents.
- Began developing a compliance training module that addresses how to write PTAs, PIAs, SORNS, and Privacy Act statements.
- Began outreach efforts to its regional offices. FEMA is providing in-person privacy awareness training, as well as training via video teleconference. FEMA has provided privacy training to personnel at the National Emergency Training Center in Emmitsburg, MD, and to the regional office in Philadelphia, PA. FEMA is also scheduled to visit regional offices in Denton, TX, and Atlanta, GA during the next reporting period.
- Began a web-based training initiative to ensure online privacy awareness training is available to all FEMA employees. A collaborative effort between the Emergency Management Institute and the FEMA Privacy Office, the goal of this program is to ensure that online privacy awareness training is available to all FEMA employees and contractors.
- Provided privacy reference materials in an electronic format rather than a hard copy format through training presentations, newsletters, and welcome e-mails to new FEMA employees regarding future privacy awareness and training efforts. The focus of these materials is privacy compliance, education and training, incident response, and mitigation.
- Participated in a forum entitled *Privacy Act – Discussion of New Routine Uses and the Process for Information Sharing*, at the Individual Assistance Emergency Support Function #6 Conference held in San Diego, CA from April 27-30, 2010.
- Published articles about safeguarding PII in several publications such as "FEMA Forward," "FEMA Weekly," and "DHS Today." FEMA will also use its employee newsletters to disseminate privacy awareness materials and educate employees on their PII responsibilities.

Looking ahead, FEMA's privacy awareness and training efforts will include completion of its effort to deliver instructor-led privacy training to all 10 regions as well as implement advanced privacy compliance training for all employees and contractors.

C. I&A

The I&A Privacy Office has begun sending privacy awareness e-mails to the I&A workforce to raise the level of awareness regarding privacy. These e-mails provide the basics of privacy principles as well as lessons learned from other agencies within the federal government. Feedback is encouraged and the hope is that these e-mails will further understanding of privacy considerations in the day-to-day operations of I&A. As noted above in Part One, Section I of this report, I&A had appointed a privacy officer at the close of the reporting period. The Privacy Office's 2011 Annual Report will provide a fuller description of I&A activities under the new privacy officer's leadership.

D. ICE

ICE is the largest investigative component agency in DHS with more than 19,000 employees in over 400 offices in the U.S. and around the world. ICE's mission is to protect the security of the American people and homeland by vigilantly enforcing the nation's immigration and customs laws. ICE's Privacy Office was established in April 2008 and now consists of four federal personnel. The office is in the process of hiring one additional federal position.

During the past year, ICE made significant progress improving compliance with the Privacy Act and E-Government Act. During the reporting period, ICE more than doubled its PIA compliance score from 30% in the third quarter of FY 2009 to 71% in the third quarter of FY 2010. ICE also issued one new SORN and published 10 updates to existing SORNs during the reporting period.

ICE published a PIA for its new Online Detainee Locator System (ODLS) on April 9, 2010.[70] ODLS is a public system available on the Internet that allows family members, legal representatives, and members of the public to locate immigration detainees who are in ICE custody. For the first time, the system makes it possible to search online for a person in civil immigration detention and determine if he or she is in custody and, if so, where. The ICE Privacy Office was involved in the development of ODLS from the earliest stages to ensure that privacy protections were incorporated into the system design. The ICE Privacy Office also participated in discussions with interested immigration and civil liberties groups on the appropriate balance between the transparency the system was intended to provide to the immigration detention process, and individual privacy concerns about the extent to which immigration detainee PII should be publicly available on a searchable database.

ICE continues to focus on raising privacy awareness among its employees and contractors. In addition to mandated annual privacy and security training, the ICE Privacy Office is providing tailored training to ICE program offices to improve their understanding of privacy laws and policies, and to provide specific guidance on the unique privacy issues faced by their office. For example, earlier this year ICE provided specialized privacy training for ICE's Office of Congressional Relations on the special legal requirements that govern disclosures of PII to Congress. The ICE Privacy Office is also in the process of integrating privacy training into existing agency training held for new supervisors and attorneys.

[70] ODLS deployed in July 2010. The ODLS PIA is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ice_odls.pdf.

Another focus for the ICE Privacy Office over the past year has been to raise external awareness about the office and its mission. The ICE Privacy Officer recently presented an overview of ICE's privacy program at the May 2010 quarterly meeting of the DPIAC. The Office has also briefed congressional staffers, and on several occasions met with non-governmental organizations interested in ICE's immigration enforcement mission.

E. S&T

During the reporting period, S&T continued to collaborate with the DHS Privacy Office to streamline the compliance documentation process and address privacy issues associated with S&T research and development projects. For example, S&T invited the DHS Privacy Office and CRCL to participate in the S&T Screening Technology Brown Bag meeting. This meeting provided a forum where the DHS Privacy Office, CRCL, and S&T Program Managers could discuss relevant privacy and civil rights issues associated with the development and implementation of screening technologies. From this meeting, S&T was able to discern broader areas and issues regarding the privacy compliance process at S&T, and address in collaboration with the DHS Privacy Office, and CRCL, where appropriate.

F. TSA

TSA was created in the wake of the terrorist attacks of September 11, 2001, and is responsible for protecting the nation's transportation systems to ensure freedom of movement for people and commerce. TSA is most visible through its airport security screening efforts at more than 460 airports, but also has security roles affecting other modes of transporting people and commodities including highways, maritime ports, rail, mass transit, and pipelines.

1. Outreach and Awareness

With over 50,000 employees at more than 460 locations, privacy awareness efforts are a significant requirement. The TSA Privacy Office took several steps aimed at maintaining privacy awareness within its employee and contractor workforce, including issuing another privacy awareness poster in its popular "Privacyman" series. The posters are designed to provide a short privacy message, and point employees and contractors to available resources for more information. TSA Privacy also institutionalized mandatory annual privacy training for all employees and contractors, and has been added as a formal reviewer for information technology services, hardware, and software acquisitions, giving the office an important insight into new systems with potential privacy impacts.

Other awareness activities included speaking at employee meetings, maintaining an internal website with privacy resources for TSA employees, and broadcasting email messages on such topics as restricting access to information in shared electronic folders, safeguarding PII, and reducing holdings of PII to reduce the impact of intrusions or loss. TSA Privacy also continued its "Privacy Awareness Press" series, issued periodically to sensitize program managers on privacy issues that received media attention.

External outreach included several speaking engagements at public conferences including the Computers, Freedom, and Privacy 2010 conference; the annual meeting of the Privacy Coalition (a consortium of 43 advocacy groups); meetings with the Liberty Coalition; and with individual privacy advocates from several organizations throughout the year. TSA Privacy also spoke to the U.S. Department of Agriculture Privacy Conference about TSA programs, and was consulted by several agencies on privacy issues affecting those agencies.

2. Programs

The Secure Flight program is designed to bring within the federal government the watchlist matching functions previously performed by the airlines. Dual benefits from the program include more consistent watchlist matching and more consistent application of redress for those passengers mistaken for individuals on a watchlist. The program began operations in early 2009 and has fully implemented domestic flight operations.

Another program with heightened public interest has been the use of Advanced Imaging Technology (AIT) to search for non-metallic threat items, including explosives, hidden on the body.[71] These technologies use millimeter wave energy or x-ray energy to highlight anomalies on the body. TSA has designed the program to provide for complete anonymity for the individual undergoing the scan by placing the officer viewing the scan in a windowless room remotely located to prevent the officer from viewing the individual undergoing the scan, disabling the capability of any machine used in an operational setting to store or retain an image, placing a blur over the face, and providing notice to individuals that they may decline the scan in favor of a physical pat-down. The physical pat-down is needed to provide a comparable level of threat detection provided by the imaging technology. TSA is working with manufacturers to develop automated functions that effectively recognize anomalies and thereby eliminate the body image created by existing technology. Implementation of the program is expected to accelerate over the coming year, with additional funding provided by Congress. AIT is being explored by a number of other countries that have performed their own privacy review.

TSA also seeks to simplify the security checkpoint experience and reduce the stress associated with air travel. To that end, TSA launched *MyTSA*, a free mobile application for members of the public seeking information on air travel, such as what items can be brought through the security checkpoint and what items can be carried inside of checked baggage. *MyTSA* is an alternative to the TSA website for providing information to the traveling public. It permits members of the public to share security checkpoint wait times, and make use of a data feed provided by the Federal Aviation Administration regarding airport delays due to weather or other factors. *MyTSA* does not collect or use PII. It will make use of the GPS features of the 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.[72]

[71] See page 59 of the 2009 Annual Report for a description of TSA's most recent update of this PIA. The report is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf.
[72] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_mytsa.pdf.

G. USCG

The Coast Guard Privacy Office was actively engaged in implementing a privacy culture and privacy protections for personal information during this reporting period.

1. Annual Information Systems Security Officer's Conference

To promote privacy awareness, Coast Guard Privacy Staff delivered a presentation at the Annual ISSO Conference in Orlando, FL on April 15, 2010. More than 150 ISSOs, Designated Approving Authorities, and Information Assurance personnel attended this week long conference. The privacy presentation provided attendees detailed information relative to identifying, preventing, and reporting privacy incidents. Presenters discussed current policies and reporting procedures. Further, additional guidance outlined ways to: 1) avoid processing set-backs; 2) ensure safeguard procedures remain in place; and 3) raise privacy awareness at their respective commands.

2. Presentation at Assignment Officers Training Workshop

During August 2009, the Coast Guard Privacy Office conducted Incident Reporting and Safeguarding PII training at the Coast Guard Assignment Officers Conference in Arlington, VA. The Assignment Officers are responsible for coordinating transfers, special assignments, separations, and retirements for 33,000 active duty and reserve Coast Guard personnel. They routinely counsel Coast Guard commands and members on various aspects of the assignment process and are instrumental in developing policies and procedures. Their duties require interfacing with various human resource systems and medical documents containing sensitive PII, to determine suitability for assignments. Pertinent information presented by the Coast Guard Privacy Staff was beneficial in creating heightened awareness regarding the importance of safeguarding PII.

3. Presentation at Headquarters Annual FOIA Training

In December 2009, the Coast Guard Privacy Staff presented an overview of the Privacy Act during the Annual FOIA Training Workshop. More than 50 Directorate FOIA Coordinators/Processors and their supervisors received in-depth information on the relationship between FOIA and the Privacy Act. Topics included Exceptions, Exemptions, Systems of Records Notices, and Civil/Criminal Penalties for non-compliance.

4. Privacy Compliance Documentation

The Coast Guard achieved significant milestones with the publication of PIAs for the National Pollution Funds Center-Pollution Response Funding, Liability, and Compensation System, the Core Accounting Suite, and the Marine Information for Safety and Law Enforcement System. In a major efficiency measure, the Coast Guard Privacy staff, together with program managers, General Counsel, Records Officer, and the DHS Privacy Office, consolidated numerous law enforcement, financial, and search and rescue missions to form three major information systems. This accomplishment not only fulfilled Coast Guard mandated and statutory requirements but continued our overall commitment to preserve public trust and promote transparency within the Department.

5. Emergency Information Collection

In response to the explosion of the Deepwater Horizon Mobile Offshore Drilling Unit in the Gulf of Mexico on April 20, 2010, the Coast Guard's Office of Information Management received OMB approval for an emergency information collection from members of the public who operate oil skimmers that could be used to aid in clean-up efforts. It was determined that the information sought, which includes PII, would be most expeditiously collected through the Coast Guard's Homeport Website. Coast Guard Privacy developed the information collection form, in consultation with Coast Guard's counsel, other Coast Guard officials (including Ocean Engineering, Operations Systems Command, Information Collection, Forms, Acquisitions, and Public Affairs), the National Incident Command (NIC) (including agencies other than DHS), and the DHS Privacy Office. Coast Guard Privacy and the DHS Privacy Office conducted a PTA for the form, outlining the overall strategy and the collection mechanism. The form includes the requisite Privacy Act Statement and also includes an opt-out button for those opposed to having their PII shared with members of the NIC other than DHS. OMB has approved the form and this initiative is ongoing.

H. USCIS

USCIS is responsible for overseeing lawful immigration to the U.S. and preserving America's legacy as a nation of immigrants while ensuring that no one who is a threat to national security or public safety receives an immigration benefit. The USCIS Office of Privacy achieved several significant accomplishments this year. A full-time Senior Privacy Compliance Specialist joined the USCIS Office of Privacy and provided support in the identification, review, and documentation of USCIS privacy-sensitive systems, programs, and operations.

The USCIS Privacy Officer issued a privacy management directive, *Handling Sensitive and Non-Sensitive Personally Identifiable Information*, informing employees and contractors of USCIS policy and procedures and their responsibilities in identifying and handling sensitive and non-sensitive PII. In addition, a privacy incident response plan was developed and implemented during the year.

During the reporting period, USCIS Office of Privacy staff conducted 23 privacy awareness training sessions for an estimated 1,800 federal employees and contractors nationwide, and nearly 9,000 employees completed the DHS Privacy Office's *A Culture of Privacy Awareness* computer-based training. In addition, new USCIS hires received privacy awareness training during new employee orientation, the USCIS Verification Privacy Branch hosted "privacy awareness month" in May, and Congressional staffers and liaisons were briefed on the process for requesting information on behalf of an individual seeking USCIS benefits. By the end of FY 2010, the USCIS Office of Privacy expects to have trained over 18,000 federal employees and contractors throughout its Regional Offices, District Offices, Field Offices, Asylum Offices, and Application Service Centers.

Finally, the USCIS Office of Privacy has been working collaboratively with the Office of Transformation Coordination, the USCIS program office responsible for agency-wide organizational and business transformation initiatives, and other key stakeholders, to ensure privacy considerations are embedded throughout the USCIS transformation process. Staff from the USCIS Office of Privacy has been actively participating in meetings and discussions of the

USCIS Transformation Leadership Team, Program Integrated Project Team, Working Integrated Project Team, Legal, Regulatory, Policy and Privacy and the Privacy Working Group to ensure privacy is integrated into USCIS programs and operations.

USCIS Verification Division

The USCIS Verification Division recently added employer business information from D&B to E-Verify to provide greater assurance that new users are actual employers. Previously, employers were not validated when they enrolled in E-Verify, which was identified as a privacy risk by the DPIAC and privacy advocacy groups. Confirming an employer's business information with a commercial data source establishes a level of identity assurance of the employer and thus minimizes the chances of fraudulent companies using E-Verify to confirm personal information for illegal purposes. Commercial data also enables the Verification Division to identify and manage duplicate registrations and provides the program with a better understanding of who their users are by allowing for real-time validation against commercial data. The addition of employer business information in E-Verify is discussed in the updated E-Verify PIA. See Part One, II.B.2 for additional discussion on the E-Verify PIA and SORN.

I. USSS

The Secret Service undertook several initiatives to continue to promote a culture of privacy. During the reporting period, a mandatory computer-assisted privacy awareness training course was offered continuously within the Secret Service's Learning Management System. Secret Service employees and contractors are required to take the course annually. In addition, instructor-led training, which covers both FOIA and the Privacy Act, was provided to new employees throughout the year at the Secret Service's Rowley Training Center.

In an effort to educate the staff at the Secret Service beyond the mandatory training course, the FOIA/Privacy Act Program also developed an intranet page to disseminate information 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, PIAs, and to meet other privacy compliance requirements.

As of this reporting period, USSS recruitment efforts for FOIA and Privacy Compliance professionals are still underway, and the FOIA/Privacy Act Program is collaborating with the USSS Personnel Office to streamline hiring by automating the review and selection process.

The Secret Service FOIA/Privacy Act Program, Systems Manager, Program and/or Project Managers, and Information Assurance Branch have also continued to identify systems requiring PTAs and PIAs. This collaborative effort continues to promote and improve transparency and privacy compliance within the Secret Service.

J. US-VISIT/NPPD

The US-VISIT Program 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.[73]

Privacy is an integral and essential part of US-VISIT. Privacy is integrated into US-VISIT, from conception through the planning, development, and execution of every aspect of the program.

Before gaining access to agency information and information systems, US-VISIT employees and contractors must complete classroom privacy training. During this reporting period, 295 new employees and contractors completed instructor-led privacy training. To ensure that employees and contractors continue to understand their privacy and security responsibilities after they are initially trained, annual privacy refresher training is delivered via a computer-assisted training program. During this reporting period, 753 employees and contractors completed the computer-based course, *A Culture of Privacy Awareness.*

The mission of the US-VISIT Privacy Office is to uphold the privacy of individuals while helping protect our nation. US-VISIT does this by adhering to the letter and spirit of U.S. privacy laws, complying with the FIPPs, treating people and their personal information with respect, and ensuring a high standard of privacy protection.

Activities during the reporting period included the following:

- On July 31, 2009, the Director of US-VISIT gave a presentation on "A Dual Mission: Identity Management and Privacy Protection in the Federal Government" at the Catalyst Conference, in San Diego, California. He discussed how US-VISIT's privacy strategies have contributed to the overall success of the program. Approximately 1,500 individuals were in attendance from industry, academia, and government.
- On September 24, 2009, US-VISIT's Privacy Officer participated in a panel session discussing the Department and US-VISIT's privacy program at the Biometrics Consortium Conference (BCC) in Tampa, Florida. The BCC is one of the premier conferences in the field of biometrics where the latest trends, research, and developments are discussed.
- From November 9-13, 2009, US-VISIT participated in discussions with international data protection professionals from Europol and the French Data Protection Authority (CNIL) held at the DHS Privacy Office.
- On January 20, 2010, US-VISIT's Deputy Assistant Director for Business Policy and Planning participated in a panel titled "Privacy Issues Fireside Chat" at the National Defense Industrial Association 2010 Biometric Conference in Arlington, Virginia. Over 250 individuals, primarily from government and industry, were in attendance.

[73] The authorities pursuant to which US-VISIT undertakes activities include the following: section 2 of the Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215, 114 Stat. 337 (June 15, 2000); section 205 of the Visa Waiver Permanent Program Act of 2000, Public Law 106-396, 114 Stat. 1637, 1641 (Oct. 30, 2000); section 414 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Public Law 107-56, 115 Stat. 271, 353 (Oct. 26, 2001); and section 302 of the Enhanced Border Security and Visa Entry Reform Act of 2002 (Border Security Act) Public Law 107-173, 116 Stat. 543, 552 (May 14, 2002) and Section 7208 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Public Law 108-458, 118 Stat. 3638, 3817 (Dec. 17, 2004)..

- On February 2, 2010, US-VISIT's Privacy Officer gave a Privacy Overview presentation to members of an Austrian delegation that included two ambassadors from the Federal Ministry for European and International Affairs and members from the Federal Chancellor's Office and the Federal Ministry of Interior.
- On April 21, 2010, US-VISIT's Privacy Officer participated in a panel session titled, "Effective Privacy Incident Lifecycle Management in U.S. Government Agencies" at the IAPP Global Privacy Summit held in Washington DC. He discussed US-VISIT's privacy program and the processes in place to prevent and address privacy incidents.
- US-VISIT created a privacy fact sheet for distribution to US-VISIT stakeholders, trade show participants, and the general public. The fact sheet highlights the importance of privacy protection at US-VISIT, lists the US-VISIT privacy principles, describes the US-VISIT mission statement, and educates the public about the redress process.
- From April 19-22, 2010, US-VISIT's Privacy Officer participated in discussions with representatives from Justice Canada and the Spanish Ministries of Interior and Justice about how US-VISIT incorporates privacy protections in its projects. These meetings are further discussed as part of the DHS Privacy Office International Exchange Program in Part Three, Section II.B.
- US-VISIT also supported the establishment of the NPPD Privacy Program and helped develop new employee training. A Privacy Analyst from US-VISIT was detailed to NPPD for 90 days to help with the initial stages of setting up the NPPD Privacy office. This individual served as the Acting Privacy Officer for NPPD, provided oversight for the Privacy program, and imparted guidance and support on a wide range of privacy issues. While at NPPD, the Privacy Analyst formulated and administered the Onboarding Privacy Overview training that is given to all new employees during orientation, worked on submitting required compliance documents, and initiated work on various PIAs.

During the reporting period, the US-VISIT privacy program also continued to demonstrate a strong commitment to privacy protection by publishing a PIA for the Five Country Conference (FCC) High Value Data Sharing Protocol (FCC Protocol), in collaboration with the DHS Privacy Office. The US-VISIT Program published this PIA to cover a new, systematic and long-term information-sharing project with trusted partner countries for immigration purposes. The FCC is a forum for cooperation on migration and border security among Australia, Canada, New Zealand, the United Kingdom (U.K.), and the United States. The FCC Protocol is a data and information sharing agreement among all the members of the FCC that is aligned with the DHS mission as well as the US-VISIT Strategic Plan. This Protocol supports immigration processes, including asylum and refugee determinations, among the FCC member countries. It allows the FCC partners to exchange biometric information in specific immigration cases where: 1) the identity of the individual is unknown or uncertain; 2) the individual's whereabouts are unknown; or 3) there is reason to suspect that the person has been encountered by one of the countries participating in this protocol.

The FCC Protocol aligns with the mission of US-VISIT to:

- facilitate legitimate travel;
- prevent immigration and identity fraud;

- identify inadmissible individuals, individuals with outstanding wants or warrants, and those convicted of certain crimes;
- identify individuals who are attempting to gain admission into or are seeking a benefit from an FCC country by fraud; and
- resolve immigration and other cases requiring identity or confirmation of an individual's location.

The United States has begun exchanging limited biometric and biographic information with Canada, the U.K., and Australia as part of the FCC Protocol. This sharing is expected to improve the integrity of the asylum system, enhancing the ability of the FCC partners to identify and prevent abuse of their respective asylum systems, and to identify individuals who may not qualify for asylum or refugee protection. Part Three, Section I of this report further discusses the FCC Protocol and PIA.

Part Two – Leading the Way: Enhancing Accountability and Transparency

The DHS Privacy Office continues to champion accountability and transparency of Department and federal government operations and to pursue an open dialogue with the public and Congress. Oversight of Department PIAs and SORNs is only one of several ways in which the Office fosters accountability and transparency. Part Two of this report discusses the varied additional paths the Office takes to further this goal: taking a proactive approach to implementing the President's Open Government Initiative; enhancing disclosure and reducing FOIA backlogs throughout the Department; ensuring that effective redress mechanisms are available to the public; and demonstrating the Office's own accountability and transparency through public and Congressional reporting.

I. Engaging the Public

The Chief Privacy Officer has made engaging the public a primary focus of her agenda for the DHS Privacy Office since her appointment in March 2009. 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 – both U.S. and international citizens.

A. Transparency and Disclosure

The DHS Privacy Office's implementation of the FIPPs begins with the principle of transparency. The Department puts this principle into practice most notably through robust FOIA and Privacy Act programs. FOIA is the codification of the right to access records in the possession and control of federal agencies at the time a request is received. All agencies within the Executive Branch are subject to the provisions of FOIA. The Act establishes a presumption that records in the possession and control of Executive Branch agencies are available to the public, except to the extent the records are subject to one or more of the Act's nine specific exemptions or three special law enforcement exclusions.

In accordance with Executive Order 13392, *Improving Agency Disclosure of Information*,[74] signed by President Bush on December 14, 2005, the Secretary designated the Chief Privacy Officer to serve concurrently as the Chief FOIA Officer. The additional responsibility for disclosure compliance was delegated to the DHS Privacy Office in recognition of the close connection between privacy and disclosure laws. Given that FOIA is a pillar of the U.S. privacy

[74] Exec. Order No. 13392, 70 Fed. Reg. 75373 (Dec. 14, 2005). See also 5 U.S.C.§ 552(k)

protection framework, the Chief FOIA Officer's oversight of both privacy management and FOIA management allows for greater transparency of DHS operations. By policy, DHS implements both FOIA and the Privacy Act uniformly and consistently to provide maximum allowable disclosure of agency records upon request. Requests processed under the Privacy Act are also processed under FOIA; requesters are always given the benefit of the statute with the more liberal release requirements.

As noted in the DHS Privacy Office's 2009 Annual Report, on January 21, 2009 President Obama issued the *Transparency and Open Government Memorandum*, which committed the Administration to an "unprecedented level of openness in government."[75] On the same date, the president issued the *FOIA Memorandum*, in which the President described FOIA as "the most prominent expression of a profound national commitment to ensuring an open government."[76] On March 19, 2009, the Attorney General established a new standard for defending agency decisions to withhold information. When a FOIA request is denied, agencies are now defended "only if (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the statutory exemptions, or (2) disclosure is prohibited by law."[77] Consistent with President Obama's memoranda and the Attorney General's memorandum, DHS FOIA offices continue to process requests with a presumption of disclosure.

During the reporting period, the DHS Privacy Office continued to lead the Department's implementation of the president's *FOIA Memorandum* and the Attorney General's implementing guidance. The Disclosure and FOIA Group issued several types of guidance on implementing the new initiative over the past year. In her capacity as the DHS Chief FOIA Officer, the Chief Privacy Officer issued memoranda to all DHS employees, implementing a policy of proactive disclosure consistent with the President's transparency initiatives and guidance on implementing the proactive disclosure policy,[78] and conducted outreach throughout the Department commemorating Sunshine Week 2010.[79] The Chief FOIA Officer also continued the dialogue among component FOIA offices related to the Administration's guidance and issued the first-ever DHS Chief FOIA Officer Report in March 2010.[80]

The Disclosure and FOIA Group's uncompromising approach to proactively disclosing information includes significant enhancements to the DHS Privacy Office FOIA Electronic Reading Room. During the reporting period, new information was posted to many of these sites on a weekly basis, thereby reducing the number of routine FOIA requests.

---

[75] *Transparency and Open Government Memorandum for the Heads of Executive Departments and Agencies*, 74 Fed. Reg. 4685 (Jan. 21, 2009), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf.

[76] *Freedom of Information Act Memorandum for the Heads of Executive Departments and Agencies*, 74 Fed. Reg. 4683 (Jan. 21, 2009), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-1773.pdf.

[77] The Attorney General's memo is available at http://www.usdoj.gov/ag/foia-memo-march2009.pdf.

[78] *Chief FOIA Officer's Memorandum, Proactive Disclosure and Departmental Compliance with Subsection (a)(2) of the Freedom of Information Act (FOIA)* (August 26, 2009), available at http://www.dhs.gov/xlibrary/assets/foia/foia_proactive_disclosure.pdf; *Chief FOIA Officer's Memorandum, Calendar Format for Proactive Disclosure* (October 30, 2009), *available at* http://www.dhs.gov/xlibrary/assets/foia/foia_proactive_disclosure_calendar_guidance.pdf.

[79] *Chief FOIA Officer's Memorandum, Freedom of Information Act and 2010 Sunshine Week* (March 16, 2010), *available at* http://www.dhs.gov/xlibrary/assets/foia/priv_foia_sunshine_week_memo_2010-03-16.pdf.

[80] *2010 Chief FOIA Officer Report to the Attorney General of the United States* is available at http://www.dhs.gov/xlibrary/assets/foia/priv_chief_foia_officer_report_cy10.pdf.

1. Proactive Disclosure

Proactive disclosure of information[81] is one of the cornerstones of President Obama's commitment to governmental transparency. In order to ensure that the Department acts in accordance with the President's openness initiative, the DHS Privacy Office issued the August 26, 2009 memorandum, *Proactive Disclosure and Departmental Compliance with Subsection (a)(2) of the Freedom of Information Act*.[82] The memorandum stresses the importance of complying with the proactive disclosure requirements of 5 U.S.C. § 552(a)(2) and directs the Department and its components to proactively post specific categories of records reflecting the Department's operations to DHS public websites. The memorandum stresses that proactive disclosure postings are to be "consistent with FOIA and other disclosure laws."

2. Intra-Departmental FOIA Compliance

During the reporting period, the Department continued working to integrate the individual component disclosure units into one cohesive DHS FOIA program. As part of the Secretary of Homeland Security's efficiency review initiative, the DHS Privacy Office led a working group that offered several recommendations on streamlining inter-Departmental FOIA processing. The Disclosure and FOIA Group continued to process FOIA requests for the DHS Headquarters programs, including the Office of the Secretary. The Director of Disclosure and FOIA also served as a liaison to DHS directorates and components, forwarding FOIA and Privacy Act requests seeking records they maintain. Additionally, the DHS Privacy Office offered FOIA and Privacy Act training to all DHS components on an as-needed basis to cultivate FOIA officers' knowledge and expertise agency-wide. The DHS Privacy Office trained approximately 250 individuals during the reporting period.

3. Reducing FOIA Backlogs in DHS Components

The Disclosure and FOIA Group continued to address FOIA backlogs across the Department while improving efforts to manage the steady increase of FOIA requests received by components. To support this effort, the Chief FOIA Officer worked with component leadership to encourage the Department's components to devote adequate resources to their FOIA programs. The DHS Privacy Office coordinated the processing of approximately 160,000 FOIA requests during the reporting year. The Chief FOIA Officer has set a backlog reduction goal of 15% for FY 2010. Further details about these initiatives will be provided in the *2010 FOIA Annual Report to the Attorney General of the United States*.[83]

4. FOIA Outreach

In addition to day-to-day interactions with the requester community, the Disclosure and FOIA Group conducts regular outreach with representatives from the information access community, as well as immigration attorneys and advocates, in the course of processing access requests. The Deputy Chief FOIA Officer and Associate Director, Disclosure Policy and FOIA Program

[81] *See Chief FOIA Officer's Memorandum* (August 26, 2009), *available at* http://www.dhs.gov/xlibrary/assets/foia/foia_proactive_disclosure.pdf.
[82] *Chief FOIA Officer's Memorandum* (August 26, 2009), *available at* http://www.dhs.gov/xlibrary/assets/foia/foia_proactive_disclosure.pdf.
[83] The 2010 Annual Report to the Attorney General of the United States covers FY 2010 and is due on February 1, 2011.

Development met with the American Immigration Lawyers Association in March 2010 to discuss matters related to both privacy and disclosure. In addition, the Associate Director, Disclosure Policy and FOIA Program Development, spoke at the 2010 Department of Justice Celebration of the Attorney General's FOIA Guidelines on March 15, 2010, to provide an overview of DHS FOIA implementation and celebrate successes in the area of transparency.

B. Open Government Initiative

OMB issued an *Open Government Directive* on December 8, 2009.[84] The Directive requires federal executive departments and agencies to take specific steps to increase transparency, public participation, and collaboration in government.[85] The Directive establishes several action items, one of which includes the drafting of an Open Government Plan. The Open Government Plan serves as a method for detailing how each department or agency will incorporate the principles of the President's January 2009 Transparency and Open Government Memorandum[86] into its mission. Among other things, the *Open Government Directive* requires that each Open Government Plan include a process for inventorying "high value" data sets that can be published online in open, downloadable formats.

DHS issued its Open Government Plan in April 2010.[87] The DHS Privacy Office provided substantial content for inclusion in the Open Government Plan and an Office staff member served on the Plan's drafting and editing team. The DHS Privacy Office plays a leading role in the Department's compliance with the *Open Government Directive* and Plan by assisting with privacy reviews of potential data sets to be posted on data.gov and USAspending.gov. The DHS Privacy Office ensures the data sets are in compliance with privacy laws, regulations, and OMB guidance before they can be posted.

1. Privacy reviews of DHS contributions to data.gov

Data.gov is a flagship effort of the Administration's Open Government Initiative. Data.gov empowers the public through easy to find, machine-usable data held by the federal government. Traditionally, federally-held data may have been difficult to find or inaccessible to the public in a usable format. The data.gov website enables the public to access downloadable federal data sets for the purpose of building applications, conducting analyses, and performing research.[88]

DHS must ensure that data sets it publishes adhere to Departmental privacy protections while at the same time providing the public with greater transparency.[89] To that end, the DHS Privacy Office reviews all proposed data sets under consideration for publication to data.gov with the OCIO Enterprise Data and Management Office during an initial review to identify data fields

[84] 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.
[85] *Id.*
[86] 74 Fed. Reg. 4685 (Jan. 26, 2009), *available at* http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf.
[87] The DHS Open Government Plan is available at http://www.dhs.gov/xlibrary/assets/dhs_open_government_plan.pdf.
[88] http://www. data.gov/about.
[89] Data.gov requires that data shared by agencies conform to all applicable security and privacy requirements including the Privacy Act, the E-Government Act, applicable federal security standards including National Institute of Standards and Technology (NIST) 800-39, and other guidance as issued by OMB (See: *Office of Information and Regulatory Affairs (OIRA) Information Policy, available at* http://www.whitehouse.gov/omb/inforeg_infopoltech.).

that might contain PII. The DHS Privacy Office then reviews more detailed information about each data set, paying particular attention to previously-identified data fields, along with sample data. Only data sets that are approved by the DHS Privacy Office are published by DHS on data.gov.

During the reporting period, the DHS Privacy Office reviewed 46 data sets, all of which were published on data.gov. These include data sets administered by FEMA, Coast Guard, the Office of Immigration Statistics, and USCIS, ranging in topic from disaster declaration summaries to refugee arrivals.

2. Privacy reviews of DHS contributions to USAspending.gov

While data.gov showcases data on a wide range of subjects, USAspending.gov focuses on annual federal government expenditures for contracts, grants, loans, and insurance. Financial reports are provided by government agencies detailing where spending is focused, to provide a broad picture of federal spending processes and to further transparency into government operations.[90]

The DHS Privacy Office reviews data sets proposed for posting on USAspending.gov for compliance with privacy laws and federal privacy policy. Only data sets that are approved by the DHS Privacy Office are published by DHS to USAspending.gov. The Office reviewed 29 data sets for 2010 DHS grants totalling over $2 billion, including grants from TSA to regional airports for electronic baggage screening programs and grants from FEMA for hazard mitigation, the National Urban Search and Rescue Response System, state fire training systems, and port security programs.

C. 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 46 privacy-related events during this past year.

1. Privacy Advocacy Community

The Chief Privacy Officer continued to host Privacy Information for Advocates meetings, her quarterly series of informational meetings with members of the advocacy community. The meetings have proven to be a useful tool for the Chief Privacy Officer to update the advocacy community on the activities of the Department and hear any privacy issues they may have.

The Chief Privacy Officer and senior members of the DHS Privacy Office also speak at various privacy-related events and fora. These fora are often hosted by advocacy groups or professional organizations, and provide another opportunity for interaction with members of the public about the DHS Privacy Office's ongoing work to implement privacy protections in a systematic manner throughout the Department. During the reporting period, the DHS Privacy Office also took the initiative to alert the privacy advocacy community by email or telephone conference calls when new reports or privacy documents of major importance are released. The Chief

[90] http://www.usaspending.gov/learn?tab=FAQ#2.

Privacy Officer views the advocacy community as an important resource in privacy policy development.

2. Federal Privacy Community

As noted earlier, the DHS Privacy Office provides leadership to the federal privacy community. This included the Privacy Committee Boot Camp (with four speakers) and Privacy Summit (with six speakers). The Chief Privacy Officer also spoke at several agency events outside of DHS (including to the IRS) in an attempt to promote best practices and systematize privacy across federal agencies. These events provide a great opportunity for DHS Privacy Staff to interact with, and learn from, their federal colleagues.

3. Privacy and Industry

On issues where there are major privacy concerns (such as identity management, social media, or cloud computing), the DHS Privacy Office staff and the Chief Privacy Officer speak at industry events to emphasize the need for building in privacy protections.

4. DHS Privacy Office Website

This year the DHS Privacy Office launched a greatly improved public website (http://www.dhs.gov/privacy). The website enhances the transparency of Office activities and provides greater ease of use and public access to Department PIAs, SORNs, and DHS Privacy Office guidance and reports. The website also features new navigation, a new home page with an intuitive roadmap making it easier to locate privacy and FOIA information, and improved, easy to scan content.

II. Complaints and Redress

Systematizing implementation of the FIPPs principle of Individual Participation throughout DHS is an essential function of the DHS Privacy Office. "Individual Participation" encompasses the concept of individual access to PII, the ability to have inaccuracies corrected, and the opportunity for other forms of redress. The Office leads the Department's privacy complaint review process, addressing complaints received by the Office itself and providing guidance to components working to address complaints addressed to them. The Office is also deeply engaged in Department efforts to improve the transparency and effectiveness of DHS redress programs. Effective complaint resolution and redress processes are integral to the Department's mission, and the DHS Privacy Office works to ensure that privacy is taken into account in their design and implementation.

A. Complaints

The DHS Privacy Office's Director of Privacy Incidents and Inquiries has responsibility for reviewing privacy complaints received by the Office, including complaints received from the general public and from non-governmental organizations. This position provides the DHS Privacy Office a dedicated resource to support complaint-handling as a team leader, team member, or sole investigator for the most difficult, sensitive, and complex privacy investigative matters.

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*, require, among other things, that the Department report quarterly to Congress on privacy complaints received and their disposition. The discussion that follows explains how complaints are categorized for FISMA reporting purposes and presents statistics for the reporting year. Additional DHS Privacy Office responsibilities under Section 803 are discussed in Part Two, Section III.A.

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.[91]

- **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.

The components and the DHS Privacy Office report disposition of complaints in one of the following 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 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.
- **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.

A cornerstone of the DHS complaint system is the definition of "complaints" set by OMB, which defines them as written allegations of harm or violation of privacy compliance requirements.[92] These reports reflect privacy complaints filed with the DHS Privacy Office and components or programs. Complaints may be from U.S. citizens and Legal Permanent Resident (LPRs), as well as visitors and aliens.[93]

The following tables provide the statistics reported to Congress and OMB during the reporting period between June 1, 2009 and May 31, 2010.[94] **Tables 2 and 3** summarize the categories and disposition of complaints received by the DHS Privacy Office and the components during the past four quarters. In the first quarter of FY 2010, the DHS Privacy Office revised the disposition of complaints to reflect a closed or an in-progress disposition. The previous reports

[91] This category excludes FOIA and Privacy Act requests for access, which are reported annually in the Annual FOIA Report.
[92] Office of Mgmt. & Budget, Executive Office of the President, OMB Memorandum No. M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008* (2008), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-09.pdf.
[93] The Department accepts complaints pursuant to the Mixed Systems Policy, which is discussed below in Part Two, Section II.B of this report
[94] The quarterly reporting period for June 1, 2010 through August 31, 2010 was on-going at the close of the reporting period for the Privacy Office Annual Report.

reflected a disposition of either responsive action taken, no action required, or pending. The data appears in 2 separate tables to reflect these changes in disposition. **Table 4** reports the total number of complaints received during this reporting period by category.

It is important to note that in the fourth quarter of FY 2009, the number of closed "process and procedure" complaints reflects 2,012 complaints received as part of a fourth quarter FY 2008 write-in campaign regarding laptop searches. The complaints sought to influence policy regarding laptop searches as opposed to individual redress. As discussed in the previous Annual Report, the complaints were identical and largely related to searches of electronic devices at the border. As discussed more fully in Part One, Sections II.B.2 and IX.A.1, the Department published the Border Searches of Electronic Devices PIA, which responded to the complaints.

Privacy Complaints Received with Action Taken

Type of Complaint	Number of Complaints	Disposition of Complaint		
		Responsive Action Taken	No Action Required	Pending
Fourth Quarter FY 2009 (June 1, 2009 - August 31, 2009)				
Process and Procedure	11	2021	2	0
Redress	256	355	0	14
Operational	49	19	1	58
Referred	49	47	0	0
Total	***365***	***2442***	***3***	***72***

Table 2: DHS Privacy Complaints Received During Fourth Quarter FY 2009

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)
First Quarter FY 2010 (September 1, 2009 - November 11, 2009)				
Process and Procedure	6	6	0	0
Redress	26	25	1	0
Operational	31	20	11	8
Referred	5	8	0	0
Total	***68***	***59***	***12***	***8***
Second Quarter FY 2010 (December 1, 2009 – February 28, 2010)				
Process and Procedure	5	5	0	0
Redress	17	18	0	2
Operational	22	15	8	18
Referred	2	2	0	0
Total	***46***	***39***	***8***	***20***
Third Quarter FY 2010 (March 1, 2010 – May 31, 2010)				
Process and Procedure	5	5	0	0
Redress	2	2	0	2
Operational	31	50	6	1
Referred	15	15	0	0
Total	***53***	***72***	***6***	***3***

Table 3: DHS Privacy Complaints Received During First –Third Quarters FY 2010

Type of Complaint	Number of Complaints	Disposition of Complaint	
		Responsive Action Taken	No Action Required
Fourth Quarter FY 2009 to Third Quarter FY 2010 (June 1, 2009 - May 31, 2010)			
Process and Procedure	27	2037	2
Redress	301	400	0
Operational	133	104	1
Referred	71	72	0
Total	***532***	***2613***	***3***

Table 4: DHS Privacy Complaints:
Total Received From Fourth Quarter FY 2009 Through Third Quarter FY 2010

2. Component Complaint Handling

Below are some examples of component responses to complaints received during the reporting period. Collaboration among the DHS Privacy Office and components was a major factor contributing to the successful resolution of these complaints.

a. CHCO

An individual reported that she received an unsealed envelope containing her health benefits information via US mail. The Chief Human Capital Officer (CHCO) PPOC investigated the issue and discovered the office had sent out a batch mailing of health benefits information to DHS employees using a glue stick and the individual's envelope had not remained sealed. The office immediately discontinued the process of mailing health benefits information to employees. Employees are now required to obtain copies of any health benefits documentation through their electronic personnel files.

b. US-VISIT

A husband and wife contacted US-VISIT regarding a biometrics issue. The issue involved a possible error in their fingerprint capture. US-VISIT reviewed the records of both individuals and confirmed that an operational error had resulted in the fingerprints of the husband being associated with the wife's biographic data, and vice versa. US-VISIT corrected the information in the system so each individual's biometric data was correctly associated thus preventing future travel problems.

An individual sent a complaint to US-VISIT regarding a biometrics issue. She stated that she had been sent to secondary screening causing her inconvenience at the airport. US-VISIT reviewed her record and discovered that the problem was incorrectly labeled finger prints. Her thumb prints were incorrectly labeled as her index finger prints on the matchers. This caused the prints that were taken on entry to mismatch against the prints on file. US-VISIT corrected her record to the traveler's satisfaction.

US-VISIT received an email from an individual who wanted to know where to send her I-94 form. For nonimmigrant visitors entering the United States with a visa, there is a requirement to complete a CBP Form I-94. This form has two specific perforated sections to it. The visitor or the carrier representative must complete both sections of CBP Form I-94 upon arrival in the United States. The bottom section of CBP Form I-94 is a departure record and must be returned

to U.S. officials upon exiting the United States. This individual had forgotten to turn in the departure record at the airport and was worried that she would be recorded as having stayed in the U.S. beyond her authorized period of admission. Since this was not a US-VISIT issue but rather a CBP issue, US-VISIT directed the individual to CBP's webpage with the relevant I-94 information.

c. CBP

CBP has taken proactive steps to make information regarding the receipt and use of PNR data, US-VISIT data collection, and the CBP inspection process more transparent by posting privacy policies, frequently asked questions, links to appropriate government websites, and fact sheets, to the public CBP website, www.cbp.gov. This information can also be obtained by contacting the call center and in tear sheets provided to interested travelers at the ports of entry.

A traveler at the Dallas Fort-Worth airport asked, "What does [sic] the CBP and the government do with the information that was entered into the system about me and what impact will it have on me in the future both in my travels personally/professionally (i.e. background checks, etc.)?" CBP responded to the traveler's e-mail with information regarding the collection of PNR and biographical data citing relevant privacy policies for both collections.

d. TSA

TSA Privacy received complaints from both the public and from TSA employees during the reporting period. Complaints from the public centered on TSA programs, generally on concerns with the AIT program, which has received significant media coverage. Many of the complaints were from individuals who had not actually experienced AIT, but had concerns based on media reporting.

One example of an AIT issue pertained to an individual who complained to a privacy advocate that AIT signage advising of the technology and option to decline AIT screening was missing at Miami International Airport. TSA Privacy Office was able to immediately contact TSA personnel in Miami to check all four of the lanes utilizing AIT at that time and not only confirm that signage was in place, but also take pictures of the signage in the lanes the individual would have taken based on flight information she provided. TSA was able to provide those pictures to the advocate to address the underlying complaint.

Several contacts from the public sought assistance with tracking applications for transportation sector credentials. Employee complaints typically involved concerns about whether workman's compensation or leave records had been appropriately shared, or expressed concern the appropriate use of Social Security Number as an identifier.

3. Improving the Complaint Handling Process

The DHS Privacy Office is continuing to upgrade and standardize its complaint handling processes. In September 2009, the Office began using its newly developed electronic Complaint Tracking System (CTS). The Chief Privacy Officer approved the required CTS PIA, dated June 29, 2009, and the CTS SORN, which was published in the *Federal Register* on July 21, 2009. CTS is an electronic correspondence workflow management system that has allowed the DHS Privacy Office to respond more effectively and efficiently to address privacy complaints, comments, and requests for redress from the public, DHS employees and contractors, other government agencies, and the private sector. CTS has aided in the compiling of quarterly data for complaints for the Section 803 reporting described previously in this section.

4. Response to Public Inquiries

In addition to complaints, the DHS Privacy Office receives hundreds of email inquiries throughout the year requesting information or providing comments. The DHS Privacy Office provides an email address through its website at privacy@dhs.gov, which members of the public use to contact the Office. The Office reviews every email received. The majority of requests for information have involved issues that are outside the DHS Privacy Office's area of responsibility. These comments, complaints, and requests are referred to the appropriate component or other federal agency for resolution.

B. Redress

Redress is a critical principle of the FIPPs and the Privacy Act, affording individuals the ability to request an update or correction to information maintained about them. Redress for U.S. persons is codified in the Privacy Act. Due to the degree with 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, which is discussed below.[95] This section discusses the redress landscape at the Department and provides examples of significant administrative redress efforts currently supported by the DHS Privacy Office.

1. Privacy Act Redress

Under section (d)(2) of the Privacy Act, an individual can request amendment of his or her own record.[96] During the reporting period, the DHS Privacy Office received no requests for amendment under the Privacy Act. The DHS Management Directorate and NPPD each received one such request, and in each case the requestor's personal information was amended.

2. Non-Privacy Act Redress

a. Mixed Systems Policy

As a matter of law, the Privacy Act provides statutory privacy rights to U.S. citizens and LPRs, 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

[95] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.
[96] 5 U.S.C. § 552a(d)(2).

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 Number 2007-1 DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons* (DHS Mixed Systems Policy).[97] 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 significance of the Mixed Systems Policy is that it directly supports the FIPPs principle of individual participation for programs such as the DHS Traveler Redress Inquiry Program (DHS TRIP), which allows for administrative redress. DHS TRIP is discussed more fully below.

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. Part Three of this report includes a complete description of these outreach activities.

b. DHS TRIP

In its third 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. The Chief Privacy Officer is a member of the DHS Trip Advisory Board. To date, DHS TRIP has received and processed over 100,000 requests for redress and has an average response time (from the time of first submission to final resolution) of approximately 60 days. The public receives three important benefits through centralized redress request processing. First, DHS TRIP is a one-stop process. The applicant is not required to know which component is responsible for addressing the request. In some cases, the agency or component with which the individual experienced the difficulty may not be the same agency or component whose information triggered the action. Consequently, DHS TRIP personnel review each case to determine which agency or component is involved and route the redress request to the appropriate agency or component. Second, DHS TRIP simplifies the redress process for travelers. Where needed, DHS TRIP enables multi-agency review of a case through a single application and interaction with the public. This process frees the applicant from the cost and burden of approaching each screening agency or component individually. Third, DHS TRIP is able to leverage the Secure Flight Program operated by the TSA, which allows the uniform prescreening of passenger information against the federal government watch list for commercial travel. [98]

[97] The DHS Mixed Systems Policy, initially issued on January 19, 2007, was revised on January 7, 2009. It is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

[98] Secure Flight is a passenger pre-screening program that transfers responsibility for the watch list matching function from the airlines to the federal government. In addition, by mandating the collection of Full Name, Gender,

DHS TRIP follows the Department's privacy policies and practices and was designed to seek only the minimum amount of PII necessary to process an applicant's request. DHS TRIP personnel have been trained to handle PII (including sensitive PII) consistent with DHS privacy policy and use IT systems that have strong IT security safeguards.

c. US-VISIT Redress Program

The US-VISIT program was established in March 2003 to accurately record the entry and exit of travelers to the U.S. by collecting biographic and biometric information (e.g., digital fingerprints and photographs). Today, US-VISIT is advancing the security of the U.S. and worldwide travel through information sharing and biometric solutions for identity management. Individuals with a complaint or concern regarding delayed or denied airline boarding, delayed or denied entry into or exit from the U.S., or a complaint that they are being continuously referred to additional (secondary) screenings may submit a redress request to US-VISIT. Redress requests may also be submitted through the DHS TRIP program and additionally by emails, fax, or mail. US-VISIT received 1250 redress requests during the period July 1, 2009 – June 8, 2010 and responded to 1,399 redress requests during the same period (including 149 pending requests from the previous reporting period). US-VISIT responded to 95% of these 1,399 requests within 20 business days. The remaining 5% took 21 business days or longer. In January 2010, US-VISIT established a new goal to provide a timely response to 99% or more of all redress requests within 20 business days. Part One, Section IX.J of this report provides additional information about US-VISIT.

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 23,710 appeals and denied 580. Additionally, TTAC granted 3,615 waivers and denied 144.

Date of Birth, and the DHS TRIP Redress Control Number (if applicable), it is expected that a reduced number of travelers will be mistaken for individuals on the watch list. In those instances, information shared by DHS TRIP enables the Secure Flight Program to quickly determine that misidentified passengers are not the persons of interest whose names are actually on the watch lists. Secure Flight is currently conducting watch list matching for all U.S. domestic flights and is in the process of assuming watch list matching for international flights, anticipating full implementation by December 2010. Thus far, results indicate that obtaining these additional data elements is indeed making a difference by permitting automated resolution of potential name matches to the watch list.

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. In addition to the reporting on complaints discussed in Part Two, Section II.A of this report, the Office issues Congressionally-mandated public reports that document progress in implementing DHS privacy policy and FOIA policy. The Office issues the Department's annual data mining report, as required by Congress. DHS Privacy Office staff members also provide briefings to the Congress on privacy and FOIA-related matters upon request. The activities discussed below demonstrate the Department's commitment to transparency and public accountability.

A. 9/11 Commission Act Section 803 Reporting to Congress

Section 803 of the 9/11 Commission Act requires quarterly reporting by select privacy offices within the federal government, including the DHS Privacy Office. Each Section 803 report contains information regarding: (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 the complaints received by the Department for alleged violations, and (4) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the Chief Privacy Officer's activities.

Section 803 of the 9/11 Commission Act established additional privacy and civil liberties reporting requirements for DHS. For the purposes of Section 803, DHS currently reports on the following activities:

- PTAs;
- PIAs;
- SORNs and associated Privacy Act Exemptions;
- Privacy Act (e)(3) Statements;
- CMAs; and
- Privacy protection reviews of IT and program budget requests, including OMB 300s and Enterprise Architecture Alignment requests through the DHS EAB.

1. Activities Reported

Table 5 provides the number of Section 803 reviews completed by DHS from June 1, 2009, through May 31, 2010, by type of review.

Type of Review	Number of Reviews
Privacy Threshold Analyses	557
Privacy Impact Assessments	79
System of Records Notices and associated Privacy Act Exemptions	67
Privacy Act (e)(3) Statements	33
Computer Matching Agreements	4
Privacy Protection Reviews of IT and Program Budget requests	108
Total Reviews Completed June 1, 2008 through May 31, 2009	**848**

Table 5: DHS Section 803 Reviews Completed June 1, 2009 through May 31, 2010

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. During the reporting period, DHS released the following guidance related to privacy:

- *DHS Privacy Office Guide to Implementing Privacy* (June 2010)
- *Privacy Impact Assessment Guidance* and Privacy Impact Assessment Template (June 2010)

From June 1, 2009, through May 31, 2010, DHS conducted the following training:

- DHS personnel and contractors attended instructor-led privacy training courses in 10,706 instances.
- DHS personnel and contractors completed computer-assisted privacy training courses in 148,446 instances.

Section 803 Reports regarding complaints received by the DHS Privacy Office and components are discussed in Part Two, Section II.A of this report. See Part One, Section VIII for further discussion on DHS Privacy Office training activities.

B. FOIA Reporting to the Attorney General and Compliance

As required by Section 552(e)(1) of FOIA, the DHS Privacy Office is responsible for submitting an annual report of Department FOIA activities to the U.S. Attorney General.[99] The 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. In February 2010, the DHS Privacy Office issued its *2009 Annual Freedom of Information Act Report to the Attorney General of the United States* (2009 FOIA Annual Report) in compliance

[99] 5 U.S.C. § 552(e)(1).

with FOIA requirements.[100] The 2009 FOIA Annual Report was published on the Office's website along with the reported data in machine-readable format.[101] Although the Office was required to post machine-readable format data only for the 2009 reporting period, it published machine-readable format data for all previous reporting periods to make the information more accessible to the public.[102]

The Office also published the Department's first Chief FOIA Officer Report in March 2010 as required by the Attorney General's March 19, 2009 *Freedom of Information Act Memorandum for the Heads of Executive Departments and Agencies*.[103] The memorandum asks agency Chief FOIA Officers to "review all aspects of their agency's FOIA administration, with particular focus on concerns highlighted in the memo, and report to the Department of Justice each year on the steps that have been taken to improve FOIA operations and facilitate information disclosure at their agencies."[104] The 2009 Chief FOIA Officer Report discusses the actions taken by the Office to apply the presumption of openness, ensure the Department has an effective system for responding to requests, increase proactive disclosures, greater utilize technology, reduce backlogs, and improve timeliness in responding to requests. The report is available on the Office's website.[105]

C. Data Mining Report to Congress

In December 2009, the DHS Privacy Office issued its 2009 Data Mining Report to Congress (2009 Data Mining Report), as required annually by the Federal Agency Data Mining Reporting Act of 2007 (Data Mining Reporting Act).[106] The Office's annual data mining reports describe DHS activities already deployed or under development that meet the Data Mining Reporting Act's definition of data mining. After working with all DHS components to review DHS activities against that definition, the DHS Privacy Office identified no new activities for inclusion in the 2009 Data Mining Report. The Report includes detailed updates on programs initially described in the Department's 2008 Data Mining Report, including (1) the Automated Targeting System Inbound, Outbound, and Passenger modules administered by CBP; (2) the Data Analysis and Research for Trade Transparency System administered by ICE; and (3) the Freight Assessment System administered by TSA.[107]

None of the programs discussed in the 2009 Data Mining Report use data mining to make unevaluated automated decisions about individuals. These programs do not make decisions about individuals solely on the basis of data mining results. In all cases, DHS employees conduct investigations to verify (or disprove) the results of data mining, and then bring their own judgment and experience to bear in making determinations about individuals initially identified through data mining activities. The DHS Privacy Office continues to work closely with each of these programs to ensure that their required privacy compliance documentation is current and

[100] http://www.dhs.gov/xlibrary/assets/foia/privacy_rpt_foia_2009.pdf.
[101] The DHS Privacy Office provided FOIA data in Microsoft Excel files online.
[102] Reports and machine-readable data files are available at http://www.dhs.gov/xfoia/editorial_0424.shtm.
[103] http://www.justice.gov/ag/foia-memo-march2009.pdf.
[104] *Id.* at 3.
[105] http://www.dhs.gov/xlibrary/assets/foia/priv_chief_foia_officer_report_cy10.pdf.
[106] 42 U.S.C. § 2000ee-3.
[107] Report is available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_datamining_2009_12.pdf.

that privacy protections have been implemented. The 2010 Data Mining Report will provide further updates on these programs as needed and will also include descriptions of any new or proposed Department activities that the DHS Privacy Office determines meet the Data Mining Reporting Act's definition of data mining.

D. Congressional Briefings

On March 18, 2010, the Chief Privacy Officer submitted a written statement for the record to the House Committee on Oversight and Government Reform, Subcommittee on Information Policy, Census, and National Archives at a hearing concerning FOIA and other disclosure initiatives. The Chief Privacy Officer detailed the DHS Privacy Office's efforts to implement policy changes in support of transparency and open government, including issuing several department-wide memoranda pertaining to FOIA, highlighting the important changes in the application of FOIA under the current Administration, and instituting a proactive disclosure policy. The testimony highlighted DHS's success in reducing its FOIA backlog, steps taken to apply the presumption of openness and increase proactive disclosures at DHS, the Department's increased utilization of technology, and steps taken to ensure that DHS has an effective system for responding to requests.

During the reporting period, the Chief Privacy Officer, DHS Privacy Office staff, and component privacy officers briefed various Congressional committee staff on a wide-variety of DHS programs and initiatives including DHS TRIP, searches of electronic media at the border, DHS Privacy Office support for the fusion center program, information sharing between DHS and the European Union, DHS cybersecurity initiatives, and the role of component privacy officers.

IV. DPIAC

The DHS DPIAC is chartered under the Federal Advisory Committee Act[108] 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 undertakes matters assigned to it by the Chief Privacy Officer and conducts its deliberations in public meetings. Its role is advisory only, and it issues its findings and recommendations in public reports. In recognition of the DPIAC's contributions to the Department since the Committee was established in 2004, Secretary Napolitano recently renewed the Committee's Charter for a two-year term ending in May 2012.

A. Meetings

During the reporting period for this report, the DPIAC held four public meetings and issued two public reports. All DPIAC reports, meeting agendas, and meeting transcripts are posted on the DHS Privacy Office website.

On September 10, 2009, the DPIAC held a public meeting in Detroit, Michigan. The meeting began, as do all DPIAC meetings, with an update from the Chief Privacy Officer on the activities of the DHS Privacy Office since the Committee last met. The DPIAC then received a series of briefings from representatives of USCIS, ICE, TSA, and CBP on DHS outreach and engagement efforts with ethnic and religious communities in the metropolitan Detroit area. While in Detroit, the DPIAC members also participated in information exchanges with representatives of Arab-American community groups and toured the Arab-American National Museum in Dearborn, Michigan. These activities provided the DPIAC members with additional insight into the impact of DHS outreach efforts directed toward the Detroit area Arab-American community. The Committee members also toured CBP facilities at the Port of Detroit, heard presentations on CBP operations there, and received a briefing on TSA's Advanced Imaging Technology screening operations at Detroit Metropolitan Wayne County Airport.

The DPIAC's next public meeting took place on December 3, 2009, in Washington, DC. Following the Chief Privacy Officer's update, the Committee heard a presentation on the DHS CTS and on the DHS Privacy Office's role in supporting DHS TRIP. The Committee also received a briefing by the Acting DHS Deputy Assistant Secretary for Policy on the role of the DHS Screening Coordination Office (SCO) in implementing the Department's core strategic objectives for screening programs and on the types of screening and credentialing programs currently in use throughout the Department. The meeting concluded with a briefing by the Acting Deputy Officer for Programs and Compliance, DHS Office for Civil Rights and Civil

[108] Federal Advisory Committee Act, 5 U.S.C. App. 2.

Liberties on CRCL's responsibilities, including its legal authorities for conducting Civil Liberties Impact Assessments (CLIA) and a description of the key inquiries undertaken in the CLIA process. The CRCL briefing also included an update on CRCL's work on a CLIA for DHS component border searches of electronic devices and on opportunities to improve processes related to those searches (e.g., training materials and notices to passengers).

On March 18, 2010, the DPIAC held a public meeting in Washington, DC. The Committee received a briefing by the DHS Deputy Assistant Secretary for Cybersecurity and Communications on computer network security and related privacy protections in DHS, including the Department's role in the CNCI (focusing on the DHS Privacy Office's work on PIAs for EINSTEIN 1, EINSTEIN 2, and the proof of concept pilot project of the EINSTEIN 1 capabilities with the U.S. Computer Readiness Team and the State of Michigan), the National Cyber Incident Response Plan (NCIRP), and the National Cybersecurity and Communications Integration Center, which will unify efforts of the National Coordinating Center, US-CERT, DHS I&A, and the National Cybersecurity Center. The Unclassified Initiative Three PIA was released the same day as the DPIAC March meeting in order to increase transparency. See Part One, Section V.A.1 for additional information on the Unclassified Initiative Three PIA. The Committee then heard a presentation on the DHS Privacy Office's participation in interagency privacy initiatives undertaken by the Federal CIO Council's Privacy Committee. See Part One, Section VII.C.1 for additional discussion on Privacy Committee activities conducted during this reporting period.

During the March meeting, the Committee deliberated upon and adopted two public reports. The first report, entitled *Elements of Effective Redress Programs* (Redress Report), provides nine recommendations on designing, implementing, and providing oversight for privacy redress programs. The recommendations incorporate the FIPPs and emphasize effective notice, timely response to, and impartial adjudication of complaints, a robust appeals process, employee training, and accountability.[109] The Committee's second 2010 report, entitled *Recommendations for the PIA Process for Enterprise Services Bus Development* (ESB Report) includes six recommendations on implementing the FIPPs in the development and deployment of an Enterprise Services Bus (ESB), the technology infrastructure that delivers data to be used for various purposes (or "services") throughout the Department. The ESB Report also includes lists of suggested questions for assessing the privacy impacts of both existing and proposed Department ESBs.[110]

The DHS Privacy Office has worked with SCO and DHS TRIP to leverage the Committee's Redress Report guidance in ongoing Department efforts to make that program more transparent and more effective for travelers. The Office plans to use the ESB Report recommendations to create a new PTA for initial privacy assessments of DHS ESBs and to create a new template PIA to standardize privacy protections in ESBs throughout the Department.

The DPIAC held another public meeting in Washington, DC, on May 25, 2010. The meeting began with remarks by DHS Secretary Janet Napolitano, who recognized the Committee's positive impact on several Department programs and thanked the Committee members for their

[109] Report No. 2010-01 (March 18, 2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_report2010_01.pdf*;* See Part Two, Section II for more on the Chief Privacy Officer's responsibilities related to redress.
[110] Report No. 2010-02 (March 18, 2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_report2010_02.pdf.

support for Department efforts to protect core American values, including privacy, while protecting the country against threats to its security. The Chief Privacy Officer provided her customary report on the work of the DHS Privacy Office before she and the Secretary answered the Committee's questions. The Committee then received a briefing on information sharing governance within DHS, including the DHS Privacy Office's reliance on the recommendations in the DPIAC's May 2009 report entitled *White Paper: DHS Information Sharing and Access Agreements*[111] to shape both Departmental guidance on information sharing agreements with external partners and the review process for those agreements. The Committee then heard presentations on implementation of DHS privacy policy by ICE and on federal interagency efforts to develop the NSTIC.

B. Future Plans

Plans are currently underway for quarterly public DPIAC meetings in the remainder of FY 2010 and in FY 2011. Each meeting will include a presentation by a component privacy officer, to give DPIAC members insight into component implementation of DHS privacy policy and to provide context for future DPIAC guidance to the Department. The DHS Privacy Office looks forward to continuing its work with various DHS programs to evaluate and address the DPIAC's recommendations.

[111] Report No. 2009-01 (May 14, 20009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_dpiac_issa_final_recs_may2009.pdf. The Report is discussed in Section III.H of the DHS Privacy Office's 2009 Annual Report to Congress *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_rpt_annual_2009.pdf

Part Three – Leading the Way: Advancing International Privacy

With such a large portion of the DHS mission encompassing international partnerships and global threats, it is not surprising that international privacy concerns have been a significant theme for the DHS Privacy Office over the last year. The DHS Privacy Office has been a clear, consistent and authoritative voice in the international privacy dialogue, reaffirming the Department's commitment to respecting the privacy of all people. Part Three of this report discusses the Office's guidance to the Department on international privacy issues and the extensive outreach conducted with the Department's international partners.

A primary mission of the DHS Privacy Office's International Privacy Policy (IPP) group is to promote international cooperation and understanding of privacy issues relevant to the Department's mission and operations. In support of the Department's activities, the IPP group:

- provides advice on international agreements related to personal information collection and sharing;
- offers educational outreach and leadership on the Department's privacy policies and emerging international privacy issues;
- interprets international data protection frameworks to aid in interaction with our foreign partners; and
- advises the Department and other agency partners on global privacy practices and policy approaches.

I. Advice on International Agreements

As the Department has increased its efforts to engage in information sharing with international partners, IPP's workload has increased in providing advice on international information sharing policy and agreements. International information sharing agreements provide the DHS Privacy Office with an opportunity to develop and promote best practices with the Department's allies and partners. During the reporting period, DHS compliance tools, such as PIAs, have been increasingly recognized by the Department's international partners as models for accountability and transparency.

Preventing and Combating Serious Crime (PCSC) Agreements

PCSC Agreements, which allow for the exchange of biometric and biographic data and are required of all 36 Visa Waiver Program (VWP) countries under the 9/11 Commission Act, are a significant advancement in cross-border information sharing. During the reporting period, the IPP group provided subject matter expertise to the Department's SCO and the VWP Office, as well as to the Departments of Justice and State, during the negotiation of several of these

agreements. While negotiation of 36 separate information sharing agreements is a multi-year process, the DHS Privacy Office is helping to develop a PIA that will support PCSC information sharing.

FCC High Value Data Sharing Protocol

Throughout the reporting period, the IPP group also supported Department efforts to implement the FCC High Value Data Sharing Protocol (FCC Protocol). Implementation of the FCC Protocol is an example of how privacy compliance documentation required in the United States by the E-Government Act is becoming an international standard. All of the FCC countries have similar requirements for privacy compliance documents, but not all have the same transparency requirements. The IPP group assisted US-VISIT and the SCO by providing subject matter expertise as they drafted the FCC Protocol privacy compliance documents. The IPP group also provided advice to the DHS Office of International Affairs on possible expansion of information sharing among the FCC partners beyond the current High Value Data Sharing Protocol. US-VISIT's work related to the FCC Protocol is discussed in Part One, Section IX.J of this report.

High Level Contact Group (HLCG)

Important efforts in cross-border information sharing with the EU are those undertaken by the HLCG. Beginning in November 2006, the Department, together with the Departments of State and Justice, engaged in discussions with the European Council Presidency and European Commission to identify "common principles" of an effective regime for privacy protection that would enable the EU and the U.S. to work more closely and efficiently together to exchange law enforcement information while ensuring that the protection of personal data and privacy are guaranteed. In October 2009, the parties culminated their work by acknowledging the completion of the so-called HLCG data privacy principles. IPP was actively involved in the completion of those principles during the reporting period. It is anticipated that the HLCG principles will form the basis of a binding international agreement between the U.S. and the EU; IPP looks forward to providing subject matter expertise when such an agreement is negotiated.

PNR Agreement

IPP continued to support oversight and review of the 2007 U.S. - EU PNR Agreement during the reporting period. On February 8 and 9, 2010, IPP, with significant support from the CBP Office of Field Operations, CBP Office of Intelligence and Operation Coordination, CBP Privacy, CBP Chief Counsel, the DHS Office of Policy, and the DHS Office of the General Counsel, hosted a delegation led by the European Commission to conduct a joint review of the 2007 U.S. - EU PNR Agreement as required by Article 4 of the Agreement. The findings from February's joint review, co-led by the Chief Privacy Officer and European Commission Director (DG JLS), were generally positive. The European Commission's report concluded that DHS was in compliance with the 2007 Agreement and would support a positive EU Parliamentary vote on ratification of that Agreement.[112]

IPP also provided extensive advice on international privacy policy and information sharing related to aviation security. In the wake of the attempted attack of December 25, 2009, the DHS Office of International Affairs brought together a working group of representatives from DHS components and offices to identify ways to improve aviation security. Topics discussed included

[112] These findings are posted on the DHS Privacy Office's public website at http://www.dhs.gov/files/publications/editorial_0514.shtm#5.

promotion of information collection and sharing as well as adoption of technologies that have the potential to impact individuals' privacy. IPP contributions to this effort included incorporation of PIAs and other compliance tools to ensure that increased aviation security measures have a minimal privacy impact.

II. Educational Outreach and Leadership

IPP supplements the Department's work to strengthen its international partnerships through speaking at international conferences or other multilateral or bilateral fora, hosting exchange visitors, and interacting with the media.

A. International Speaking Opportunities

IPP staff spoke at various international venues in order to increase international awareness of the Department's privacy practices and to stay abreast of international trends in privacy policy. The DHS Privacy Office's participation ensures that DHS is a part of the international privacy dialogue and is influential in policy-making.

Secretary Janet Napolitano's keynote speech before the International Conference of Data Protection and Privacy Commissioners on November 4, 2009 in Madrid marked the year's most significant international outreach. The Secretary stressed the need to incorporate the FIPPs into international information sharing agreements and highlighted the U.S. Government's focus on transparency and accountability. The DHS Privacy Office participates annually in the Conference and is recognized by this body as an official observer.

Other notable international outreach during the reporting period included the following:

- A presentation to Mexican Ministry of the Interior officials on the U.S. privacy framework in the context of export security. The Mexican Ministry of the Interior is working on export control legislation and sought input from the U.S. government and U.S. legal experts on export controls.
- A presentation to the Corporate Data Protection and Privacy Compliance Conference in the U.K., on the U.S. Model of Privacy Oversight in the Public Sector. This included meetings with the U.K. Ministry of Justice and Home Office officials to discuss data privacy and U.S.-EU information sharing matters.
- A report before the Organization for Economic Cooperation and Development (OECD) meeting in Paris on DHS Privacy Office development of best practices on Web 2.0 use, to demonstrate the relevance of the principles memorialized in the OECD Guidelines to U.S. public sector practice.
- A presentation to the 3rd International Conference on Ethics and Policy of Biometrics and International Data Sharing in Hong Kong on the U.S. privacy framework, DHS privacy policy and practices, and on practical application of privacy best practices.
- A presentation at the February 2010 Asia Pacific Economic Cooperation (APEC) Electronic Commerce Steering Group meeting in Hiroshima, Japan, on the Department's implementation of the APEC Privacy Framework.

- The Chief Privacy Officer spoke on DHS Data Protection and Retention at the Data Protection and Data Retention Conference in Amsterdam in March 2010.

B. International Exchange Program

The DHS Privacy Office continued its international Privacy Exchange Program during this reporting year. The program is an effective means of demonstrating the U.S. privacy framework and how it governs DHS's privacy policy. Participants meet with representatives from the DHS Privacy Office, privacy officers from other DHS program offices and components, the DHS Inspector General's Office, the Department of State Privacy Office, and with other U.S. government agencies with privacy oversight responsibilities, such as the Government Accountability Office and OMB. The DHS Privacy Office hosted two exchange programs during the reporting period:

- From November 9-13, 2009, the Office hosted officials from Europol and the French Data Protection Authority (CNIL); and
- From April 19-22, 2010, the Office hosted officials from Justice Canada, the Spanish Ministries of Interior and Justice, and the German Ministry of Interior.

The DHS Privacy Office also supported a State Department-hosted International Visitor Program for European Union officials entitled "Data Privacy and Principles," which also included presentations by the US-VISIT and USCIS Privacy Officers.

C. International Media Outreach

As part of the DHS Privacy Office's public outreach, the Chief Privacy Officer published a number of articles and engaged in several media events to raise awareness of the pivotal role of privacy in DHS programs and initiatives:

- *New International Privacy Principles for Law Enforcement and Security* – The Privacy Advisor, January-February 2010 (recognizing the achievement of the U.S.-EU High Level Contact Group's completion of the HLCG Data Privacy Principles).
- *Privacy Issues in Border Searches of Electronic Devices* – Data Protection Law and Policy, October 2009 – In response to DHS's recently published directives regarding circumstances in which DHS officers can search travelers' computers and other electronic media at U.S. ports of entry, this article discusses how DHS protects the privacy and civil liberties of all travelers.
- During March and June 2010 official trips to Europe, the Chief Privacy Officer participated in several media events to answer questions and dispel myths about DHS privacy policies and practices in general and those specific to the 2007 U.S.-EU PNR Agreement.
- In June 2010, the Chief Privacy Officer met with European journalists at the State Department's Foreign Press Center to explain the U.S. privacy framework, the role of the DHS Privacy Office, and privacy protections embedded within DHS programs.

D. Additional Outreach with International Stakeholders

Throughout the reporting period, IPP engaged with foreign counterparts through formal speaking engagements at international conferences and during briefing sessions with foreign officials in the U.S. and abroad. The purpose of this engagement is to ensure that from the working level to the senior level, DHS partners are aware of the Department's privacy policies and their practical implementation. During the reporting period for this report, IPP made approximately 352 contacts with foreign entities. For example:

- IPP supported an Office of International Affairs coordinated visit by Members of the European Parliament on October 26, 2009 in Washington, DC. The Parliamentarians, members of the LIBE Committee that emphasizes Fundamental Human Rights, received briefings by the Chief Privacy Officer, US-VISIT, TSA, and the DHS Policy Office.
- On October 30, 2009, the Deputy Chief Privacy Officer and IPP met to discuss data protection in post-Lisbon Treaty Europe with the Italian Parliamentarian, who emphasized the need to factor in the influence of EU Parliamentarians.
- In November 2009, Secretary Napolitano asked the Chief Privacy Officer to support her during meetings in Madrid, London, and Brussels, to explain the U.S. privacy framework and DHS privacy policies and practices during ministerial meetings.
- In November 2009, the Chief Privacy Officer and Deputy Chief Privacy Officer met with the Dutch, Polish, and German Data Protection Authorities in Washington, DC to discuss developments in U.S.-EU information sharing and the impact privacy issues have on such sharing in the law enforcement and national security contexts.
- At Secretary Napolitano's direction, the Chief Privacy Officer travelled to Ottawa, Canada in December 2009 to meet with the Canadian Ministry of Justice, Public Safety Canada, and the Office of the Privacy Commissioner to inform them about DHS privacy policies and address misperceptions about cross border information sharing and the Information Sharing Environment.

To raise awareness of the privacy protections for the 2007 U.S.-EU PNR Agreement, the Chief Privacy Officer undertook two multi-country trips to Europe during the reporting period:

- In March 2010, to Brussels, Belgium; Strasbourg, France; Amsterdam and The Hague, Netherlands; and Berlin, Germany.
- In June 2010, to Warsaw, Poland; Budapest, Hungary; and Prague, Czech Republic.

During these visits, the Chief Privacy Officer met with European Commission officials to discuss outcomes of the February 2010 joint PNR Review and the way forward. She also met with numerous Members of the European Parliament to further explain DHS's data privacy policies regarding the PNR Agreement and to discuss the European Parliament's plans to vote on the Agreement. Her meetings with Ministries of Justice, Interior, and Foreign Affairs, and Data Protection Authorities focused on answering questions and dispelling myths on DHS privacy policies and practices while learning more about Member States' practical application of privacy principles. The Chief Privacy Officer also conducted public outreach via multiple interviews, press roundtables, and public discussions. The consistent themes of both trips included questions about the availability of judicial redress in the United States, the utility of PNR, privacy

protections associated with PNR, and the prospects for a binding U.S.-EU agreement on data privacy.

Throughout the reporting period, the DHS Privacy Office participated in interagency efforts to engage the European Commission's Justice and Home Affairs (JHA) directorate by contributing to multiple U.S.-EU JHA meetings. Issues considered during these meetings included next steps for the HLCG, including a way forward to resolve the redress principle by conducting a workshop with various stakeholders, and the U.S.-EU PNR Agreement.

III. Interpreting International Data Protection Frameworks

IPP works through several multilateral fora to participate in the international dialogue on privacy and to better understand trends in international privacy policy. During the reporting period, the DHS Privacy Office continued to participate in the OECD as a member of the Working Party on Information Security and Privacy (WPISP). The WPISP develops policy options to sustain trust, information security, and privacy in the global networked society. The WPISP's work has served as a foundation for developing national coordinated policies on privacy and data protection. The IPP group has been an active contributor to the WPISP's Global Privacy Dialogue, a series of high level events and a paper commemorating the 30th anniversary of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

For the first time, the IPP group attended as an observer during the annual plenary meeting of the Council of Europe Consultative Committee of Experts to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Adopted by the Council of Europe in 1981, Convention 108 is the only legally binding international agreement on data privacy. It has been ratified by most of the Council's 42 member countries, including all of the EU member states. The work of the Consultative Committee, which includes representatives from Justice and Interior Ministries as well as national data protection authorities, is an important forum on EU privacy policy. The DHS Privacy Office looks forward to observing future meetings.

Throughout the reporting period, IPP participated as a member of the U.S. Technical Advisory Group (TAG), which represents the U.S. in the International Organization for Standardization (ISO) Privacy Steering Committee. The TAG efforts are aimed at limiting ISO work to the technical standards within its mandate and preventing advancement of policy-based standards that would encroach on countries' existing legal frameworks.

The Department has increased its engagement with Canada, as information sharing with our northern neighbor is central to effective border management. Throughout the reporting period, the Office supported DHS in its efforts to enhance its relationship with the Government of Canada by raising awareness of U.S. privacy laws and DHS privacy policies and practices to improve effective information sharing.

IV. Advice on Department Practices and Other Agency Policy Approaches

Many countries use privacy policy to advance broader foreign policy objectives. Throughout the reporting period, IPP worked to raise the awareness of Department personnel, as well as international experts in other U.S. Government departments, on the emergence of privacy as a foreign policy issue and the need to explain the U.S. privacy framework. The DHS Privacy Office worked with the DHS Office of International Affairs, the State Department, and the Justice Department on strategies to advance U.S. privacy practices as a means of protecting individuals' personal information and building trust with foreign partners.

For example, on December 1, 2009, IPP briefed the DHS VWP Team on DHS Privacy Office functions, oversight responsibilities, and international outreach. The VWP team is part of the PCSC negotiating team, which has faced resistance because of perceived privacy and data protection concerns. The briefing was meant to make the VWP team more familiar with DHS privacy policy and to offer the DHS Privacy Office's support in future negotiations where privacy and data protection may be an issue. PCSC Agreements are discussed above in Part Three, Section I.

As interest in DHS privacy practices increased, the DHS Privacy Office staff increased support to DHS and State Department personnel posted in U.S. embassies. When traveling overseas, IPP staff met with U.S. Embassy personnel to increase their awareness of privacy as a foreign policy issue and answer any questions or concerns they may have about DHS privacy policies and practices. As discussed earlier in Part One, Section VIII.A.2 of this report, the DHS Privacy Office is currently working with the DHS Office of International Affairs and DHS components to integrate international privacy training into all outbriefings for Department attachés and liaisons posted overseas. The training will raise awareness among DHS personnel of privacy sensitivities in foreign countries and alert them to potential legal and policy issues associated with personal information and international information sharing.

Throughout the reporting period, IPP provided support and guidance on international data privacy issues for senior DHS leadership. This included reviewing and preparing materials for senior leadership international travel and meetings with foreign officials concerning DHS programs and policies regarding information sharing and data privacy.

The Future of Privacy at DHS

Throughout its history, the DHS Privacy Office has made great strides in operationalizing privacy protections throughout DHS; the past year has been no exception. As a result the culture of privacy at DHS, while still growing, is firmly planted and bearing tangible fruit. The installation of component privacy officers is a significant step forward in ensuring that privacy considerations are consistently and authoritatively addressed in the development stage of Department initiatives, which, in turn, allows for more complete and robust privacy protections to be implemented.

In the coming year, the DHS Privacy Office anticipates particular challenges in the areas of cybersecurity, fusion centers, social media, international information sharing, and other areas. The Office also expects to build its capacity to conduct targeted training, investigate incidents and inquiries, conduct privacy oversight, and ensure accountability. In addition, the Office will continue to support new and innovative ways to provide transparency and to facilitate public engagement.

The DHS Privacy Office will continue to lead the charge to institute effective privacy protections and operationalize privacy throughout the Department. Further, the Office will maintain its leadership role in privacy development across federal fora, while continuing to serve as a resource for information, guidance, and consistent policy approaches within the Department. As new and challenging privacy issues continue to arise that crosscut each of these areas, the DHS Privacy Office will continue to meet each with unmatched expertise, and unswerving commitment. By leveraging existing approaches to privacy issues, particularly the use of the FIPPs, the Office will continue to lead the way in developing privacy protective solutions for social media, cloud computing, information sharing environments, and a host of other initiatives. The goal of engaging and addressing privacy and disclosure issues in a comprehensive manner will benefit the Department, the federal enterprise, and our interactions abroad.

Appendices

A. DHS Implementation of the FIPPs

DHS's implementation of the FIPPs[113] is described below:

- **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.

[113] *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.

B. Published PIAs

The table below lists all published PIAs between July 1, 2009 and June 30, 2010.

Component	Name of System	Date Approved
DHS Wide	Privacy Complaint Tracking System	7/2/2009
S & T	Radical Rhetoric	7/12/2009
FEMA	FEMA Grants Program	7/15/2009
ICE	eBonds	7/15/2009
TSA	WBI-Update	7/23/2009
DHS Wide	e-Recruitment Update	7/31/2009
DHS Wide	QHSR	7/31/2009
ICE	General Counsel Electronic Management System Update	7/31/2009
TSA	HRAccess Program	7/31/2009
DHS Wide	Our Border	8/7/2009
ICE	Fugitive Case Management System	8/11/2009
TSA	TSA Credential Authentication Technology / Boarding Pass Scanning System Update	8/13/2009
USCIS	E-Filing	8/24/2009
USCIS	Reengineered Naturalization Casework System	8/24/2009
USCIS	eCISCOR	8/25/2009
CBP	Collection of Information during the Course of Border Search, Detention, and Seizure of Electronic Devices	8/27/2009
FEMA	National Emergency Family Registry and Locator System	8/27/2009
ICE	Visa Security Program Tracking System	8/28/2009
ICE	National Child Victim Identification System	9/1/2009
TSA	e-Law Enforcement Officer Logbook Program	9/1/2009
ICE	Federal Protective Service Information Support Tracking System (FISTS) Contract Suitability Module	9/2/2009
S & T	Critical Infrastructure Change Detection Update	9/8/2009
USCG	Marine Information System and Law Enforcement System	9/8/2009
ICE	Federal Protective Service Dispatch and Incident Record Management Systems	9/16/2009
ICE	FPS Guard Contracting Reform Rulemaking	9/16/2009
ICE	FPS Information Support Tracking System	9/16/2009
ICE	Livewave CCTV PIA	9/17/2009
USCG	Core Accounting Suite	9/21/2009
USCIS	Customer Relationship Interface System Update	9/21/2009
OIG	Investigative Records System	9/23/2009
USCG	Case Manager Management Tool	9/29/2009
ICE	IDOCX	10/14/2009
ICE	287 (g) Program Database	10/21/2009
USCIS	Travel and Employment Authorization Listings	11/2/2009
US-VISIT	Five Country Joint Enrollment and Information-Sharing Project	11/2/2009
USCG	Boating Accident Report Database	11/12/2009
Ethics	Financial Disclosure Management program Confidential Financial Disclosure Report	11/25/2009
ICE	Password Issuance and Control System	11/25/2009

Component	Name of System	Date Approved
Office of Health Affairs	Antiviral Distribution	12/1/2009
USCG	Recruit Analysis and Tracking System	12/1/2009
USCIS	Refugees, Asylum, and Parole System / Asylum Pre-Screening System	12/4/2009
ICE	Student & Exchange Visitor Information System II	12/10/2009
TSA	Alien Flight Student Plan update	12/14/2009
DHS Wide	Stakeholder Engagement Initiative: Microsoft Dynamics CRM	12/22/2009
ICE	Bond Management Information System Web Version (BMIS Web)-Interface and Collection Update	12/23/2009
ICE	Enforcement Integrated Database (EID)	1/14/2010
ICE	ICEGangs Database	1/15/2010
ICE	Child Exploitation Tracking System (ICE-CETS)	1/19/2010
S&T	Sensor Web	1/20/2010
Office of Under Secretary for Management	IdeaFactory	1/21/2010
OPS	Haiti Social Media Disaster Monitoring Initiative	1/21/2010
FLETC	Enterprise Security System (ESS)	1/25/2010
USCG	Academy Information System	1/26/2010
OPS	2010 Winter Olympics Social Media Event Monitoring Initiative	2/10/2010
ICE	Suspension and Debarment Case Management	2/19/2010
NPPD	EINSTEIN 1: Michigan Proof of Concept	2/19/2010
I&A	Intelligence Production and Dissemination Suite	3/10/2010
NPPD	US-CERT: Initiative Three Exercise	3/18/2010
CISOMB	CIS Ombudsman Virtual Ombudsman System of Records	3/19/2010
USCIS	USCIS Background Vetting Service	3/29/2010
TSA	Workplace Violence Prevention Program	3/30/2010
NPPD	Integrated Common Analytical Viewer Sensitive But Unclassified	3/31/2010
USCIS	Eligibility Risk and Fraud Assessment Testing Environment	4/9/2010
ICE	Alien Criminal Response Information Management System (ACRIMe)	4/23/2010
ICE	Data Analysis & Research for Trade Transparency System	4/28/2010
USCIS	Customer Identity Verification System Update	4/29/2010
OPS	April 2010 BP Oil Spill Response Social Media Event Monitoring Initiative	4/30/2010
ICE	Online Detainee Locator System	5/4/2010
CRCL	Civil Rights and Civil Liberties Matters	5/6/2010
NPPD	Malware Lab Network	5/7/2010
ICE	Exodus Accountability Referral System	5/13/2010
ICE	Hiring Information Tracking System	5/14/2010
S&T	First Responder Technologies	5/25/2010
USCIS	E-Verify Use of Commercial Data for Employer Verification	6/2/2010
CRCL	Equal Employment Opportunities Eagle Program	6/3/2010
USCG	Coast Guard Headquarters Security and Safety Computer Network	6/16/2010
DHS Wide	Accessibility Compliance Management System	6/22/2010
OPS	Publicly Available Social Media Monitoring and Situational Awareness Initiative	6/22/2010
DHS Wide	Digital Mail Pilot Program	6/25/2010

C. Published SORNs

The table below lists all SORNs published in the Federal Register between July 1, 2009 and June 30, 2010.

Component	Name of System	Date Published in the Federal Register
DHS Wide	**DHS/ALL-028,** Complaints Tracking System (74 FR 35877)	7/21/2009
ICE	**DHS/ICE-005,** Trade Transparency Analysis and Research (74 FR 39083)	8/5/2009
FEMA	**DHS/FEMA-004,** Grants Management Information Files (74 FR 39705)	8/7/2009
ICE	**DHS/ICE-003,** General Counsel Electronic Management System (74 FR 41914)	8/19/2009
FEMA	**DHS/FEMA-008,** Disaster Recovery Assistance Files (74 FR 48763)	9/24/2009
FEMA	**DHS/FEMA-001,** National Emergency Family Registry and Locator Systems (74 FR 48767)	9/24/2009
DHS Wide	**DHS/ALL-004,** General Information Technology Access Account Records 3 (74 FR 49882)	9/29/2009
ICE	**DHS/ICE-012,** Visa Security Program Tracking System (74 FR 50228)	9/30/2009
DHS Wide	**DHS/All-001,** Freedom of Information Act and Privacy Act (74 FR 55572)	10/20/2009
OIG	**DHS/OIG-001,** Audit Training Tracking System	10/20/2009
OIG	**DHS/OIG-002,** Office of Inspector General (OIG) Investigations Data Management System (IDMS) (74 FR 55569)	10/28/2009
ICE	**DHS/ICE-013,** Alien Medical Records (74 FR 57688)	11/9/2009
USCG	**DHS/USCG-060,** Homeport Biennial (74 FR 57692)	11/9/2009
ICE	**DHS/ICE-009,** External Investigations (75 FR 404)	1/4/2010
USCIS	**DHS/USCIS-010,** Asylum Information and Pre-screening (75 FR 409)	1/5/2010
ICE	**DHS/ICE-001,** Student and Exchange Visitor Information system (75 FR 412)	1/5/2010
DHS Wide	**DHS/ALL-024 -** Department of Homeland Security Facility and Perimeter Access Control and Visitor Management (75 FR 5609)	2/3/2010
DHS Wide	**DHS/ALL-025,** Department of Homeland Security law Enforcement Authority in Support of the Protection of Property Owned or Occupied by the Department of Homeland Security (75 FR 5614)	2/3/2010
DHS Wide	**DHS/ALL-023,** Department of Homeland Security Personnel Security Management (75 FR 8088)	2/23/2010
DHS Wide	**DHS/ALL-027,** History of the Department of Homeland Security (75 FR 8092)	2/23/2010
ICE	**DHS/ICE-007,** Law Enforcement Support Center (LESC) Alien Information Management (ACRIMe) (75 FR 8377)	2/23/2010
TSA	**DHS/TSA-023,** Workplace Violence Prevention Program (75 FR 8096)	2/23/2010
ICE	**DHS/ICE-006,** Intelligence Records Support Center (IIRS) (75 FR 9233)	3/1/2010
TSA	**DHS/TSA-006,** Correspondence and Matters Tracking Records (75 FR 18863)	4/13/2010
TSA	**DHS/TSA-013,** Federal Flight Deck Officer Record System (75 FR 18860)	4/13/2010
TSA	**DHS/TSA-011,** Transportation Security Intelligence Service Operations Files (75 FR 18867)	4/13/2010
CISOMB	**DHS/CISOMB-001,** CIS Ombudsman Virtual Ombudsman System (75 FR 18857)	4/13/2010
ICE	**DHS/ICE-011,** Immigration Enforcement operational Records System (ENFORCE) (75 FR 23274)	5/3/2010
TSA	**DHS/TSA-001,** Transportation Security Enforcement Record System (75 FR 28042)	5/19/2010
TSA	**DHS/TSA-002,** Transportation Security Threat Assessment System (75 FR 28046)	5/19/2010
USCIS	**DHS/USCIS-011,** E-Verify (75 FR 28035)	5/19/2010

D. Acronym List

Acronym List	
AILA	American Immigration Lawyers Association
AIT	Advanced Imaging Technology
APEC	Asia Pacific Economic Cooperation
ASAP	American Society of Access Professionals
C&A	Certification and Accreditation
CBP	U.S. Customs and Boarder Protection
CCTV	Closed Circuit Television
CFO	Chief Financial Officer
CHCO	Chief Human Capital Officer
CIO	Chief Information Officer
CIPP/G	Certified Information Privacy Professional/Government
CISO	Office of the Chief Information Security Officer
CLIA	Civil Liberties Impact Assessment
CMA	Computer Matching Agreement
CONOPS	Concept of Operations
CNCI	Comprehensive National Cybersecurity Initiative
CPSC	Consumer Product Safety Commission
CRCL	Civil Rights and Civil Liberties
CRE	Computer-Readable Extract
CSO	Chief Security Officer
D&B	Dun & Bradstreet
DARTTS	Data Analysis and Research for Trade Transparency System
DHS	Department of Homeland Security
DIB	Data Integrity Board
DOJ	Department of Justice
DPIAC	Data Privacy and Integrity Advisory Committee
EAB	Enterprise Architecture Board
EACOE	Enterprise Architecture Center for Excellence
EOC	Enterprise Operations Center
EU	European Union
FACA	Federal Advisory Committee Act
FEMA	Federal Emergency Management Agency
FICAM / ICAM	Federal Identity, Credential, and Access Management
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FOIA	Freedom of Information Act
FR	Federal Register
FTC	Federal Trade Commission
FY	Fiscal Year
HLCG	High Level Contact Group
HVDSP	High Value Data Sharing Protocol
I&A	Office of Intelligence and Analysis
IAPP	International Association of Privacy Professionals
ICE	U.S. Immigration and Customs Enforcement
IPC	Interagency Policy Council
IPP	International Privacy Policy
IPT	Integrated Project Team
ISCC	Information Sharing Coordination Council

Acronym List	
ISE	Information Sharing Environment
ISGB	Information Sharing Governance Board
ISO	International Organization for Standardization
ISSM	Information System Security Manager
ISSO	Information Systems Security Officers
IT	Information Technology
IRS	Internal Revenue Service
LPR	Legal Permanent Resident
NARA	National Archives and Records Administration
NPPD	National Protection and Programs Directorate
NSTIC	National Strategy for Trusted Identities in Cyberspace
OCIO	Office of the Chief Information Officer
ODLS	Online Detainee Locator System
OECD	Organization for Economic Cooperation and Development
OGC	Office of General Counsel
OIA	Office of International Affairs
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPA	Office of Public Affairs
ISGB	Information Sharing Governance Board
PCSC	Preventing and Combating Serious Crime
PGC	Privacy Guidelines Committee
PIA	Privacy Impact Assessment
PIHG	Privacy Incident Handling Guidance
PII	Personally Identifiable Information
PM–ISE	Program Manager for the Information Sharing Environment
PNR	Passenger Name Record
PPOC	Privacy Point of Contact
PRA	Paperwork Reduction Act
Privacy Act	Privacy Act of 1974
PRB	Program Review Board
PTA	Privacy Threshold Analysis
S&T	Science and Technology Directorate
SAR	Suspicious Activities Reporting
SCO	Screening Coordination Office
SORN	System of Record Notice
SSA	Social Security Administration
SSN	Social Security Number
TIC	Trusted Internet Connection
TRIP	Traveler Redress Inquiry Program
TSA	Transportation Security Administration
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
WPISP	Working Party on Information Security and Privacy