Department of Homeland Security

Privacy Office

2012 Annual Report to Congress

September 2012

Homeland Security

"We work hard 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. Privacy is embedded into the lifecycle of DHS programs and systems to inform departmental policy making and to ensure effective privacy protections."

— Mary Ellen Callahan, former DHS Chief Privacy Officer

Message from the Acting Chief Privacy Officer

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's (DHS Privacy Office or Office) 2012 *Annual Report to Congress*. This report highlights the achievements of my predecessor, Chief Privacy Officer Mary Ellen Callahan, and the DHS Privacy Office staff, during the period from July 2011 through June 2012.

Ms. Callahan, who served DHS with distinction from March 2009 to August 2012, recently returned to the private practice of law. She has left a legacy of the highest standard for professionalism, achievement and commitment to furthering the DHS mission in a privacy-protective manner, as demonstrated by this report.

The accomplishments of the past year—many the culmination of previous years of effort—clearly demonstrate the **I**nnovation, **I**nfluence, **I**ntegration, **I**mplementation, **I**nspiration, and **I**mpact that have made the DHS Privacy Office the premier federal privacy office in the United States, and a leader throughout the Federal Government community and around the globe.

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

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

The Honorable Joseph I. Lieberman
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Susan M. Collins
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

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

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

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

The Honorable Saxby Chambliss
Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Peter T. King
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Darrell Issa
Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings
Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Lamar Smith
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable John Conyers, Jr.
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Mike Rogers
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

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

Inquiries about this report may be directed to the DHS Privacy Office at 202-343-1717 or *privacy@dhs.gov*. This report and other information about the Office are available on our website, *www.dhs.gov/privacy*.

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

Executive Summary

The Department of Homeland Security (DHS or Department) Privacy Office's (DHS Privacy Office or Office) mission is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. This report, covering the period from July 1, 2011 through June 30, 2012, catalogues the Office's continued success in safeguarding individual privacy while supporting the DHS mission.

During the reporting period, the DHS Privacy Office revised its Fiscal Year (FY) 2012–2015 Strategic Plan to ensure alignment with the Department's core missions, as delineated in the Quadrennial Homeland Security Review (QHSR). The revised Strategic Plan outlines the Office's five strategic goals:

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

During the Strategic Plan revision process, the Chief Privacy Officer modified the organizational structure of the DHS Privacy Office to ensure alignment with, and accountability for, these strategic goals.

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

Goal 1: Policy

- Developed the Department-wide Directive 110-01, *Privacy Policy for Operational Use of Social Media*, which was issued by the Department in June 2012. This Directive ensures that DHS incorporates privacy protections into its use of social media to carry out its authorized mission.
- Provided leadership and privacy subject-matter expertise in DHS's ongoing evaluation of its information sharing with the National Counterterrorism Center (NCTC).
- Leveraged the expertise of the Data Privacy and Integrity Advisory Committee (DPIAC). During the reporting period, the DPIAC held three public meetings and issued a public report entitled *Privacy and Technology Recommendations for a Federated Information-Sharing System*.

Goal 2: Advocacy

- Worked with Transportation Security Administration (TSA) leadership and other DHS stakeholders to design real-time, risked-based aviation screening initiatives that incorporate privacy protections and appropriate oversight mechanisms.
- Participated as a key member of the negotiating team for the 2012 U.S.-EU Passenger Name Record (PNR) Agreement. The new PNR Agreement maintains the integrity of the PNR program while providing enhanced privacy protections for travelers.

- Continued to play a vital role in the federal interagency community through active participation and leadership roles in the Information Sharing and Access Interagency Policy Committee, the Federal Chief Information Officer Council Privacy Committee, and other key interagency fora and initiatives.
- Promoted awareness and robust public dialogue on vital privacy issues through the DHS Privacy Office Speakers Series and participation in myriad events aimed at educating and engaging the federal workforce, the advocacy community, and the public on privacy-related topics.
- Reconfigured the DHS Freedom of Information Act (FOIA) website to maximize usability. The reorganized DHS online FOIA library—a key component of the site—brings together documents by type (such as directives, instructions, frequently requested records, etc.) and now includes a link requesters can use to check the status of their FOIA requests.
- Ensured that DHS personnel are provided with appropriate training regarding the privacy implications of their daily work, including launching a new mandatory annual online training course on DHS privacy policies and practices.
- Issued congressionally-mandated public reports that document progress in implementing DHS privacy and FOIA policy, as well as providing briefings to the Congress on privacy and FOIA-related matters upon request.

Goal 3: Compliance

- Approved 76 new or updated Privacy Impact Assessments (PIA) and 21 System of Records Notices (SORN), resulting in a Department-wide Federal Information Security Management Act privacy score of 82 percent for required IT system PIAs, and 95 percent for SORNs.
- Issued a Directive and Instruction on Computer Matching Agreements (CMA) and formally established a Data Integrity Board (DIB) to oversee CMAs as required by the computer matching provisions of the *Privacy Act of 1974* (the Privacy Act).
- Reviewed 176 intelligence products and 421 Intelligence Information Reports.
- Received 909 FOIA requests and processed 895 during the reporting period. Beginning in June 2012, the DHS Privacy Office also deployed specialists to the DHS Components to help them achieve processing efficiencies and reduce their FOIA backlog.

Goal 4: Oversight

- Expanded its use of Privacy Compliance Reviews (PCR) at DHS, completing five public PCR reports covering a range of programs including cybersecurity, information sharing, and the Department's use of social media.
- Conducted two investigations that led to findings of non-compliance with DHS privacy policy. One of these investigations involved a Component's use of social media for operational purposes without appropriate oversight or protections for the collection and use of personally identifiable information (PII). The results of this investigation formed the basis for the Department-wide Directive, *Privacy Policy for Operational Use of Social Media*. The purpose of the second investigation was to determine whether a DHS Component's information sharing pilot with an external agency was in compliance with DHS privacy and information sharing policy and the Privacy Act.
- Revised and reissued the *DHS Privacy Incident Handling Guidance* (PIHG), the foundation of privacy incident response at the Department, to streamline the guidance provided and incorporate lessons learned since 2007, when the PIHG was first published. During this reporting period, 683 privacy incidents were reported to the DHS Security Operations Center, a 34 percent increase from the last reporting period. The Department investigated, mitigated, and closed 598 (88 percent) of those privacy incidents.

Goal 5: Workforce Excellence

- Worked diligently to contain costs and identify savings wherever possible. During this reporting period, DHS Privacy Office management focused on sustainable and efficient use of resources, such as expanding opportunities for in-house or no-fee training, minimizing reliance on contractor support, and reducing costs associated with office space.
- Facilitated three professional development workshops for Office staff focusing on the DHS Performance Management Core Competencies of Leadership, Communication, and Teamwork/Cooperation.
- Implemented the DHS Privacy Office Internal Rotational Assignment Program. This program provides specialized skill and leadership development opportunities for Office employees.

As this report demonstrates, the DHS Privacy Office is a mature organization that both embodies and advances its vision of being a global leader in promoting and protecting privacy and transparency as fundamental principles of the American way of life. In the coming year, the Office will continue to innovate in privacy and disclosure policy, influence through effective advocacy, integrate privacy and FOIA compliance, implement privacy oversight, inspire workforce excellence, and impact Component privacy programs and operations.

Homeland Security

Privacy Office 2012 Annual Report to Congress

Table of Contents

Table of Contents

Legislative Language

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

6 U.S.C. § 142 (Privacy Officer)

(a) Appointment and responsibilities-

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

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

Background

The Department of Homeland Security (DHS or Department) Privacy Office's (DHS Privacy Office or Office) mission is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. This report, covering the period from July 1, 2011 through June 30, 2012, catalogues the Office's continued success in safeguarding individual privacy while supporting the DHS mission.

Statutory Framework and the Fair Information Practice Principles

The *Homeland Security Act* charges the DHS Chief Privacy Officer with primary responsibility for ensuring that privacy considerations and protections are comprehensively integrated into all DHS programs, policies, and procedures.[1] The Privacy Act and the *Freedom of Information Act* (FOIA) both require DHS to be transparent in its operations and use of information relating to individuals. In light of this symbiotic relationship between privacy and transparency, the DHS Chief Privacy Officer is also the Chief FOIA Officer for the Department.

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

Figure 1: DHS Privacy Office Implementation of the FIPPs

The DHS Privacy Office incorporates these universally-recognized principles into privacy and disclosure policy and compliance processes throughout the Department.

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

[1] 6 U.S.C. § 142

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

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

2012 Strategic Realignment

During the reporting period, the DHS Privacy Office revised its Fiscal Year (FY) 2012–2015 Strategic Plan (Strategic Plan) to ensure alignment with the Department's core missions, as delineated in the Quadrennial Homeland Security Review (QHSR). The QHSR affirms that "America must remain open for business and exchanges with the world, must remain true to its principles of privacy, civil rights, and civil liberties, and must be welcoming of lawful visitors and immigrants."[4] The Strategic Plan advances the Office's vision of establishing itself as a global leader in promoting and protecting privacy and transparency as fundamental principles of the American way of life.

The work of the DHS Privacy Office primarily supports three core DHS missions: preventing terrorism and enhancing security; securing and managing our borders; and safeguarding and securing cyberspace. Additionally, through training, outreach, and participation in program development and key Department agreements, the Office advances the QHSR goal of maturing and strengthening the homeland security enterprise. The revised Strategic Plan outlines the Office's five strategic goals:

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

During the Strategic Plan revision process, the Chief Privacy Officer modified the organizational structure of the DHS Privacy Office to ensure alignment with, and accountability for, these strategic goals. The Office reorganization established new teams aligned with each of the five strategic goals, delegated supervisory responsibilities among existing senior staff, and created new leadership opportunities. The realignment became effective on February 20, 2012. Figure 2 depicts the new organizational structure of the Office.

[4] The QHSR outlines the Department's homeland security strategic framework. *See Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (February 2010), at 24, available at *http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.*

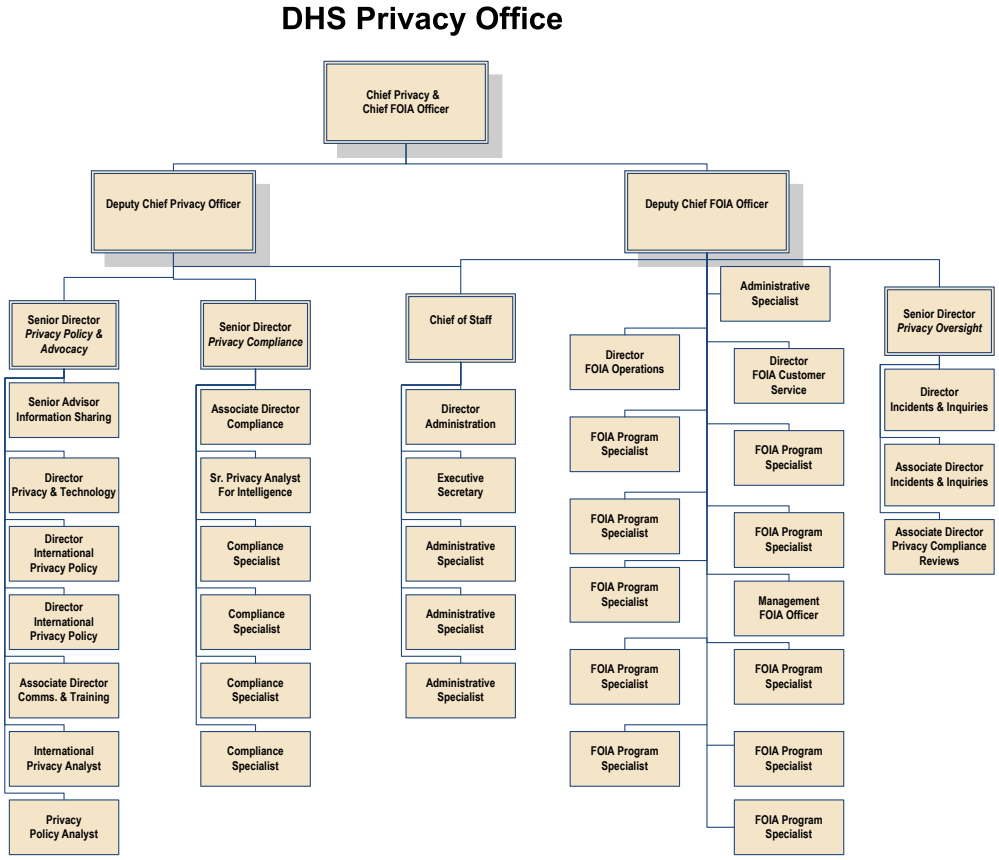


Figure 2: DHS Privacy Office Organizational Chart

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

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

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

The newly-instituted *Privacy Oversight Team* combines many pre-existing Office activities into a single unit dedicated to implementing accountability and continuous improvement of DHS privacy processes and programs. Its responsibilities include conducting Privacy Compliance Reviews (PCR) and investigations, managing privacy incidents, and providing response and redress for privacy complaints.

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

The revised Strategic Plan, and the resulting Office reorganization into the teams delineated above, will better enable the DHS Privacy Office to *innovate* in privacy and disclosure policy, *influence* through advocacy and outreach, *integrate* compliance, *implement* privacy oversight, and *inspire* excellence in our workforce. The organization of this report mirrors the Office's new organizational structure and includes contributions from Component Privacy Offices, demonstrating the practical *impact* of proactive privacy policy and protections on DHS operations.


CALENDAR
DAILY
SCHEDULE
ANN
TO DO
ON
OFF
TEL
USERFILE
MEMO
EXPENSE
CLOCK
GET
SEND
SYNC
MENU
NEW
EDIT
Q
W
E
R
ALARM

Innovation

I. INNOVATE in Privacy and Disclosure Policy

As in previous years, the DHS Privacy Office continues to address novel and complex policy issues while instilling privacy protections and transparency mechanisms into every aspect of DHS operations. The complexity of DHS operations, and the diversity of its missions, consistently propel the Office to develop innovative privacy policies and processes. This section highlights the Office's development and support of new policy initiatives to further privacy and transparency at DHS during the reporting period.

DHS's Use of Social Media

Government use of social media to communicate with, and discover information about individuals, raises privacy and transparency challenges. During the reporting period, the DHS Privacy Office provided transparency into the Department's use of social media through three mechanisms:

- The DHS Chief Privacy Officer testified before the House Committee on Homeland Security Subcommittee on Counterterrorism and Intelligence regarding the Department's use of social media on February 16, 2012. The testimony addressed the purposes for which DHS uses social media and the privacy protections embedded in those activities.[5]
- The DHS Privacy Office published reports on three Privacy Compliance Reviews (PCR) conducted to examine both the Department's use of social media for external communications and outreach to the public, and the use of social media for situational awareness by the National Operations Center.[6] These PCRs, conducted in collaboration with the National Operations Center, enabled the Office to ascertain if prescribed privacy protections were in place and to make recommendations to strengthen those protections. Section IV of this report includes more information on PCRs.
- The DHS Privacy Office developed the Department-wide Directive 110-01, *Privacy Policy for Operational Use of Social Media*,[7] which was issued by the Department in June 2012. This Directive ensures that DHS incorporates privacy protections into its use of social media to carry out its authorized mission. The Directive and the associated Instruction detail specific steps Components must take before engaging in the operational use of social media. These steps include documenting the authority to engage in the operational use of social media, providing annual training to Department employees authorized to use social media, and creating specific authority-based rules of behavior for engaging in the operational use of social media.

The DHS Privacy Office continues to ensure that privacy standards are embedded in all uses of social media throughout the Department, and are consistently applied in compliance with Directive 110-01.

Privacy Compliance Directive and Instruction

In July 2012, the Department issued Directive 047-01, *Privacy Policy and Compliance*, which formalizes long-standing DHS privacy policy and practice in the DHS Directives System. DHS Privacy Office staff drafted the Directive in consultation with Component Privacy Officers and PPOCs. The Directive and its accompanying Instruction detail the Chief Privacy Officer's role in establishing, implementing, and enforcing Department privacy policy. They also describe the privacy-related responsibilities of DHS personnel and the processes in place to ensure compliance with applicable laws, Federal Government-wide policies, and DHS privacy policy. The Directive and Instruction are made available to the public through the Department's online FOIA Library.[8]

[5] *http://www.dhs.gov/ynews/testimony/20120216-1a-priv-ops-social-media.shtm.*
[6] *http://www.dhs.gov/files/publications/gc_1284657535855.shtm.*
[7] The Directive and Instruction are posted on the Department's online FOIA Library at *http://www.dhs.gov/xfoia/gc_1254501589035.shtm.*
[8] *http://www.dhs.gov/xfoia/gc_1254501589035.shtm#0.* Since 2009, DHS has published the Department's Directives in the DHS FOIA Library.

Information Sharing Policy Leadership

During the reporting period, the DHS Privacy Office collaborated with Component Privacy Offices, the DHS Office of Intelligence and Analysis (I&A),[9] the Office for Civil Rights and Civil Liberties (CRCL), DHS Component data stewards, and external sharing partners to ensure that the Department executes its information sharing programs in a privacy-protective manner. Through these collaborative relationships, the Office:

- *Provided leadership and privacy subject-matter expertise in DHS's ongoing evaluation of its information sharing with the National Counterterrorism Center (NCTC).*
  - NCTC is the primary organization in the United States Government for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism possessed or acquired by the United States Government. The DHS Privacy Office has maintained a leadership role in DHS's engagement with NCTC for the past several reporting periods.
  - In March 2012, the Attorney General of the United States approved guidelines that, among other things, allow NCTC to retain temporarily U.S. Person[10] records that do not contain terrorism information for up to five years. These new guidelines have a potential impact on five existing Information Sharing Access Agreements (ISAA) between DHS and NCTC that limit temporary retention of U.S. Person information to 180 days. The guidelines permit DHS, and other data source agencies, to negotiate Terms and Conditions of ISAAs transferring data to NCTC, including retention periods and other privacy protections. Working through the DHS Internal Records Group—discussed in more detail below—the DHS Privacy Office and other DHS information sharing stakeholders are evaluating whether, and under what conditions, the Department should renegotiate the existing ISAAs to permit a longer temporary retention period.

[9] The DHS Undersecretary for I&A is the chair of the DHS Information Sharing and Safeguarding Governance Board and the Department's designated Information Sharing Executive.

[10] Executive Order 12333 defines a U.S. Person as a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

- *Maintained an active leadership role in DHS's internal information sharing governance processes.*
  - In July 2011, the DHS Chief Privacy Officer was designated as a voting member of the DHS Information Sharing and Safeguarding Governance Board (ISSGB),[11] the senior steering committee and policy-making body for information sharing practices at DHS. In addition to the Chief Privacy Officer's participation on the ISSGB, DHS Privacy Office staff also serve as action officers for the Information Sharing Coordination Council (ISCC), which supports the ISSGB and develops policy recommendations and guidance.
- *Reviewed and created privacy protections for DHS ISAAs.*
  - In coordination with the ISCC, the DHS Privacy Office participated in reviews of ISAAs to ensure compliance with DHS privacy policies and ISCC guidance. This included ISAAs with federal, state, local, territorial, and tribal partners.
  - DHS established a Records Working Group (RWG) to evaluate complex information sharing questions and represent the Department while negotiating ISAAs with the intelligence community and other information sharing partners. The RWG is chaired by an I&A representative in support of the I&A Under Secretary's role as Information Sharing Executive Agent at DHS. The DHS Privacy Office plays a key role in this group, together with CRCL and the Office of the General Counsel (OGC). Component data stewards are also members of the RWG.

Fusion Center Support

Section 511(a) of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[12] (9/11 Commission Act) requires CRCL and the DHS Privacy Office to provide training on privacy, civil rights, and civil liberties to all DHS officers and intelligence analysts before they deploy to state and major urban area fusion centers (fusion centers) and to support the training of all fusion center personnel nationwide on these same issues. CRCL and the Office have partnered with the I&A's State and Local Program Office (SLPO)—the office within I&A that is the focal point for DHS support for fusion centers nationwide—and the Department of Justice's (DOJ) Bureau of Justice Assistance to develop and deliver this training program.

During this reporting period the DHS Privacy Office:

- Continued participating in the Department's senior-level Fusion Center Advisory Group. The work of this group was folded into a newly created DHS Fusion Center Executive Steering Committee. The DHS Privacy Office's continued membership on this committee helps ensure Department- and USG-wide support for, and an awareness of, the Office's work to establish a strong privacy protection framework within fusion centers across the nation;
- Coordinated training, oversight, and other interactions with fusion centers by working with the SLPO;

[11] This body was previously known as the Information Sharing Governance Board or ISGB.
[12] 42 U.S.C. § 2000ee-1(f).

- In collaboration with CRCL, provided on-site training for 19 fusion centers in Alaska, Colorado, Connecticut, Illinois, Iowa, Louisiana, Minnesota, Oregon, Pennsylvania, Tennessee, Virginia, Wisconsin, and the District of Columbia to complement the comprehensive, state-specific training delivered by each fusion center's privacy officials. Additional in-person training sessions are planned at eight more centers during the remainder of calendar year 2012; and
- Participated in the National Fusion Center Conference for the fifth consecutive year. DHS Privacy Office senior staff participated in a panel entitled, *Are You Following Your Privacy Policy? The Importance of Privacy Policy Implementation*.

Disclosure and Transparency Policy Initiatives

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

- *Government Openness: The Department of Homeland Security applies both the letter and spirit of the Freedom of Information Act*,[13] issued in January 2012, reminds staff that DHS operates with a presumption of disclosure and does not assert FOIA exemptions to prevent embarrassment of public officials, possible revelations of errors or failures, or in response to speculative or abstract fears. The memorandum also reaffirms that FOIA exemptions should be applied only where the deciding official reasonably foresees that release of the requested information would harm an interest protected by one of the FOIA exemptions, or where release is prohibited by law.
- *DHS Freedom of Information Act Policy Guidance*,[14] issued in March 2012, implements new DOJ recommendations on referrals, consultations, and interagency coordination for FOIA requests that involve responsive records that originated with another agency or entity, or where another agency or entity has an interest in the records.[15] The memorandum encourages DHS Components to leverage opportunities to more efficiently handle consultations with other agencies or entities by sharing documents electronically, or by establishing guidelines or agreements to expedite the process.

Data Privacy and Integrity Advisory Committee

The DHS Data Privacy and Integrity Advisory Committee (DPIAC) provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to PII, as well as data integrity and other privacy-related matters.[16]

The DPIAC held three public meetings during the reporting period. At each meeting, the Chief Privacy Officer updated the Committee on DHS Privacy Office activities. In addition:

- During the July 11, 2011 meeting, DHS Deputy Secretary Jane Holl Lute provided an update on DHS International Information Sharing Programs, and the National Programs and Protection Directorate (NPPD) Privacy Officer briefed the Committee on NPPD's implementation of DHS Privacy Policy;

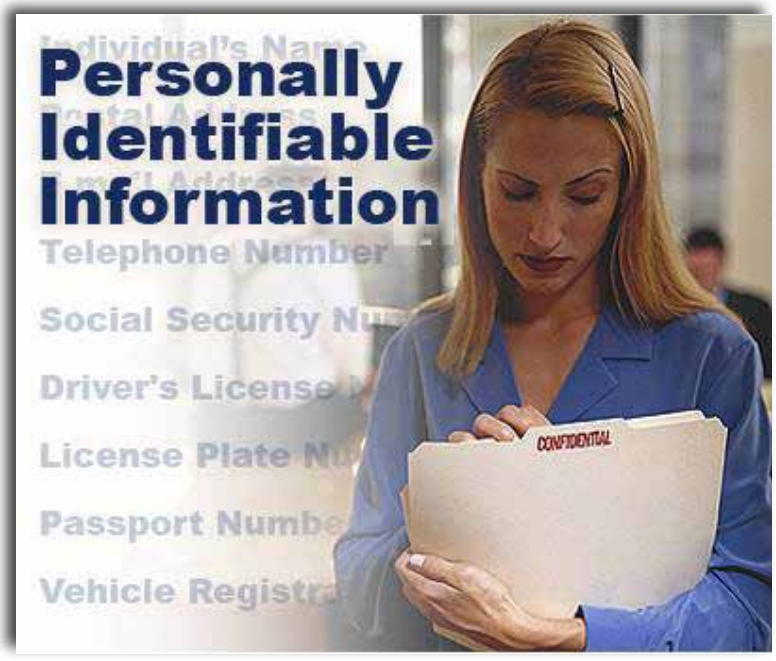
[13] *http://www.dhs.gov/xlibrary/assets/foia/foia-government-openness-memo-january-2012.pdf*
[14] *http://www.dhs.gov/xlibrary/assets/foia/dhs-foia-handling-guidance.pdf*
[15] See *http://www.justice.gov/oip/foiapost/2011foiapost42.html*
[16] The committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. § 451 and operates in accordance with the provisions of the Federal Advisory Committee Act (FACA) (5 U.S.C. App 2). DPIAC members serve as Special Government Employees and represent a balance of interests on privacy matters from academia, the private sector (including for-profit and not-for-profit organizations), state government, and the privacy advocacy community. The DPIAC provides advice on matters assigned to it by the Chief Privacy Officer and conducts its deliberations in public meetings.

- During the October 5, 2011 meeting, the DHS Deputy FOIA Officer provided an update on DHS FOIA activities, and the Transportation Security Administration (TSA) Privacy Officer provided an update on the privacy protections that have been built into the Department's use of Automated Targeting Recognition software; and
- During the December 6, 2011 meeting, the I&A Privacy Officer provided an update on I&A's implementation of DHS Privacy Policy.

On December 6, 2011, the Committee issued a public report entitled *Privacy and Technology Recommendations for a Federated Information-Sharing System*. The report analyzes privacy risks and potential benefits raised by federated information-sharing systems, and provides recommendations to the Department for building privacy protections into the design of such systems.

In May 2012, Secretary of Homeland Security Janet Napolitano approved renewal of the DPIAC Charter, which governs the work of the Committee, for a period of two years. The Charter was filed with Congress, as required by the Federal Advisory Committee Act, on May 8, 2012, and will expire on May 8, 2014. Secretary Napolitano also appointed eight new DPIAC members on May 11, 2012, bringing the current DPIAC membership to 24.

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



Influence

II. INFLUENCE through Advocacy and Outreach

Advocating for forward-leaning privacy and disclosure policies in all DHS operations is at the forefront of the DHS Privacy Office's mission. DHS privacy professionals work side-by-side with DHS operational personnel and their counterparts at other federal agencies to shape programs and embed privacy protections and proactive disclosure policies into the activities, dialogue, and products of the entire homeland security enterprise.

Privacy Leadership and Collaboration within DHS

Within the Department, the DHS Privacy Office's leadership and collaboration with the Components influences the scope and direction of programs that rely on personal information. DHS Privacy Office staff engage with Component personnel at every stage of program development to ensure privacy and transparency considerations are appropriately evaluated and integrated into Department activities. Examples of such engagements during the current reporting period are provided below.

- *DHS Law Enforcement Shared Mission Community (LE-SMC).* The LE-SMC—a working group organized under the DHS ISCC—consists of personnel from all DHS law enforcement Components and offices. DHS Privacy Office staff co-chair a working group within the LE-SMC engaged in evaluating the sharing of biometric information with state and local law enforcement partners. The Office's engagement within the LE-SMC has helped ensure the LE-SMC achieves its goal of providing relevant and timely information in support of its law enforcement mission, delivered to the appropriate state and local law enforcement users, while protecting individual privacy.
- *TSA Risk-Based Aviation Screening.* The DHS Privacy Office worked with TSA leadership and other DHS stakeholders to design real-time, risked-based aviation screening initiatives that incorporate privacy protections and appropriate oversight mechanisms.
- *Cybersecurity.* The DHS Privacy Office maintained close collaboration with NPPD and its Office of Privacy, as well as other federal cybersecurity partners, to provide ongoing privacy subject-matter expertise for cybersecurity initiatives, including the EINSTEIN program.

International Engagement and Outreach

International cooperation is integral to the success of DHS, and the DHS Privacy Office is a key player on the Department's international negotiating teams. Ensuring protection of PII in international information sharing is a key area of the Office's international activities. Cross-border sharing of PII must comply with the DHS Federal Information Sharing Environment (ISE) Privacy and Civil Liberties Protection Policy and other DHS policies. By advancing Department privacy compliance practices to international partners and promoting the FIPPs, the Office builds the confidence necessary for cross-border information sharing and cooperation.

"The DHS Privacy Office was a key member of the negotiating team for the 2012 U.S.-EU Passenger Name Record Agreement, which provides enhanced privacy protections for travelers."

U.S. - EU Passenger Name Record (PNR) Agreement. One of the most significant international information sharing achievements for the Department during this reporting period and the last several years was completion of the 2012 U.S.-EU PNR Agreement. The Chief Privacy Officer was a key member of the negotiating team, led by the DHS Deputy Secretary. The new Agreement, which supersedes the provisional 2007 Agreement,[17] maintains the integrity of the PNR program while providing enhanced privacy protections for travelers. The new Agreement features a retention period that is narrow and tailored to specified types of crime, with PII viewable in an active database for only six months. The new Agreement also provides for a new method of data transmission: "real-time" push from the airlines. By restricting data transmission to the minimum necessary, while ensuring data accuracy, the real-time push method of sharing data should enhance both security and privacy protection. Privacy impacts of the Agreement will be evaluated through regular joint reviews that will look at, among other topics, onward transfer and the use of the "push" system for collecting PNR.

U.S.- Canada Shared Vision for Perimeter Security and Economic Competitiveness (Perimeter Vision). The Chief Privacy Officer and the DOJ Chief Privacy and Civil Liberties Officer successfully led and concluded negotiation of Joint Privacy Principles, as called for in the *Perimeter Vision* declared by President Obama and Canadian Prime Minister Harper in February 2011.[18] The Principles will inform and guide information and intelligence sharing under the Beyond the Border Action Plan, which sets out joint *Perimeter Vision* priorities. DHS Privacy Office staff are an integral part of the teams drafting the Beyond the Border information sharing initiative and will ensure that immigration, travel, and law enforcement information sharing programs are consistent with the Principles.

Due to the growing breadth and depth of information sharing with Canada, DHS and DOJ have engaged in a dialogue throughout the reporting period with Public Safety Canada and Justice Canada on our respective approaches to information sharing. The DHS Privacy Office has also responded directly to inquiries from Canadian counterparts on best practices for incorporating privacy in their organizational structures. The Canada Border Services Agency (CBSA) used materials provided by the DHS Privacy Office in support of its proposal for a CBSA Chief Privacy Officer. In addition, the FOIA Team and the United States Customs and Border Protection (CBP) FOIA staff hosted a meeting with representatives from CBSA on best practices for FOIA request procedures and disclosure policies.

[17] The 2007 Agreement did not receive ratification by the European Parliament. As a matter of good faith and out of respect for our EU partners and their evolving political structures following enactment of the Lisbon Treaty, Secretary Napolitano subsequently agreed to negotiate a new agreement provided the new text would not degrade the operational effectiveness of the 2007 Agreement and would permit additional security enhancements where necessary.

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

Other International Information Sharing Initiatives. The Department participates in several additional ongoing multilateral and bilateral engagements with the goal of improved information sharing, among other objectives. These are opportunities for the DHS Privacy Office to engage with international partners on best practices for good stewardship of personal information, especially for immigration and border security matters. During the reporting period, the Office led or supported engagements in the following areas:

- **U.S.-EU Data Privacy and Protection Agreement.** The Chief Privacy Officer and staff continued to support the U.S. interagency talks with the European Commission to achieve a binding umbrella agreement with baseline standards for protecting PII exchanged for law enforcement, criminal justice, and public security purposes.
- **The Five Country Conference (FCC).** The United States hosted this year's FCC Plenary, planning the agenda for migration and border security cooperation discussions among the representatives of Australia, Canada, New Zealand, the United Kingdom, and the United States. The DHS Privacy Office continues to work with the DHS Office of Policy to imbed privacy best practices into the FCC work program, and is promoting the establishment of joint privacy principles to guide information sharing programs currently under development.
- **International Conference of Data Protection and Privacy Commissioners.** The Chief Privacy Officer and DHS Privacy Office staff participated in the 33rd annual Conference, which was hosted by Mexico. The Chief Privacy Officer engaged in dialog with privacy supervisory authorities during panels on *Privacy by Design in the Public Sector and Data Protection Agency Oversight of Privacy at Law Enforcement Agencies*. Office staff also participated on a panel called *Balancing Privacy and Recovery in a Natural Disaster.*
- **International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee on Information Technology–Security Techniques.** The DHS PIA template has been accepted by this international standards-setting body as a model for development of a generic, standard PIA. The DHS Privacy Office contributed the PIA template through the U.S. Department of Commerce, National Institute for Standards and Technology (NIST), the United States coordinator for this forum.
- **Organization for Economic Cooperation and Development and Organization of American States.** The DHS Privacy Office continued to support interagency engagement with these two multilateral organizations in their privacy guidelines drafting initiatives. The Office has advocated for positions consistent with U.S. policies and practices in areas such as information sharing, breach notification, and effective oversight.

International Training and Outreach. Outreach to our international partners increases understanding of the U.S. privacy framework and advances DHS privacy practices as a model. As information sharing has become more prevalent in the Department, the DHS Privacy Office has taken a lead role in instituting training of DHS and other United States Government officers involved in information sharing programs, including officers deployed overseas. For example, during this reporting period:

- **U.S. Department of State Foreign Service Institute (FSI)**. FSI is the Federal Government's primary training institution for officers of the U.S. foreign affairs community. The DHS Privacy Office staff, through coordination with the Federal Chief Information Officer (CIO) Council Privacy Committee, developed an international privacy policy training module for the existing FSI orientation course. The DHS Chief Privacy

Officer presented during the first training module on January 12, 2012, providing Foreign Service Officers with an overview of international privacy policy issues and current events in both the public and private sectors.

- **"DHS 201" International Attaché Training.** DHS Privacy Office staff participated in the development of training, entitled "DHS 201," for DHS employees who take on new roles as DHS attachés at U.S. Embassies worldwide. The Office created an international privacy policy module to raise awareness among new attachés of the potential impact of global privacy policies, and to inform them of DHS privacy policy along with resources to support their overseas objectives. The first official training program was held in August 2012, and will be conducted regularly thereafter for all outgoing attachés.

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

Interagency Leadership

Cultivating and sustaining a leadership role in the federal privacy community is a key objective for the DHS Privacy Office's efforts to promote privacy and openness throughout the homeland security enterprise. During the reporting period, the Office continued to play a vital role in the federal interagency community through active participation and leadership roles in key interagency fora and initiatives.

Information Sharing and Access Interagency Policy Committee (ISA-IPC). The ISA-IPC is the primary federal interagency body devoted to information sharing policy development for national security. The ISA-IPC is co-chaired by the White House National Security Staff and the Program Manager for the ISE in the Office of the Director for National Intelligence. Through its participation in the ISA-IPC, the DHS Privacy Office has maintained its leadership role in advancing privacy protections through the development of sound information sharing policies, both within DHS and across the Federal Government.

The Privacy Office serves on the following subcommittees and working groups of the ISA-IPC:

Privacy and Civil Liberties Subcommittee – The DHS Chief Privacy Officer is the current chair, and a member of the standing Executive Committee, of the ISA-IPC Privacy and Civil Liberties Subcommittee, the body that issues ISE Privacy Guidelines and manages their implementation. Office staff also support the following Subcommittee working groups:

- *Privacy and Information Technology Working Group.* A senior DHS Privacy Office staff member serves as chair of this working group, which developed a process for members of the interagency community to request and receive advisory opinions from the Subcommittee on privacy and civil liberties issues related to information sharing.
- *Legal Issues Working Group.* Office staff participated in this group, which analyzes and advises the Subcommittee on concerns relating to the implementation of the ISE Privacy Guidelines.

- **Fusion Centers Subcommittee** – This Subcommittee is designed to help the fusion centers achieve the four critical operational capabilities of (1) receiving information; (2) analyzing this information through a formal risk assessment process; (3) disseminating threat information; and (4) gathering locally-generated information. For each capability, DHS Privacy Office staff worked to implement privacy and civil liberties protections.
- **Suspicious Activity Reporting (SAR) Subcommittee** – DHS Privacy Office staff participate in this Subcommittee, which is responsible for overseeing the National Suspicious Activity Reporting Initiative.
- **Information Integration Subcommittee** – This Subcommittee addresses issues related to data aggregation processes across the federal community. DHS Privacy Office staff provide privacy expertise and guidance to the Data Aggregation Working Group of this Subcommittee.

The Federal CIO Council Privacy Committee.[19] The Chief Privacy Officer continued to serve as co-chair of the Federal CIO Council Privacy Committee, the principal interagency forum to improve federal agency practices for the protection of privacy. The Privacy Committee serves as the interagency coordination group for Senior Agency Officials for Privacy and Chief Privacy Officers in the Federal Government. It provides a consensus-based forum for the development of privacy policy and protections throughout the Federal Government by promoting adherence to the letter and spirit of laws and best practices advancing privacy.[20] DHS Privacy Office staff supported the following subcommittees and Privacy Committee initiatives:

- **Best Practices Subcommittee** – Senior DHS Privacy Office staff co-chairs this Subcommittee with the Federal Deposit Insurance Corporation. The Subcommittee continued its work on several projects intended to enhance privacy protections throughout the Federal Government, including the first ever appendix of privacy controls for NIST Special Publication 800-53, *Recommended Security and Privacy Controls for Federal Information Systems and Organizations (Rev. 4) (SP 800-53)*, which NIST is currently revising following a period of public comment. NIST expects to release the final version of SP 800-53 in late 2012 or early 2013.
- **Identity Management (IdM) Subcommittee** – DHS Privacy Office staff co-chairs this Subcommittee with the Social Security Administration (SSA). The IdM Subcommittee has been an active contributor this year to numerous Open Government initiatives and is particularly active in efforts relating to the ongoing development of the *Federal Identity, Credential and Access Management Roadmap and Implementation Guidance*.
- **International Privacy Subcommittee** – DHS Privacy Office staff led Subcommittee efforts to organize an international privacy policy seminar for United States Government employees, entitled *Privacy Worldwide: An Introduction to the Global Privacy Debate*. Seminar speakers, including the former DHS Deputy Chief Privacy Officer, addressed global privacy policy issues to raise awareness among public sector agencies, and to promote a unified strategy when addressing misperceptions about the U.S. privacy framework or advancing U.S. privacy policy abroad. DHS Privacy Office staff also contributed significantly to the Subcommittee's goal of establishing international privacy policy training for federal employees through the FSI, as discussed under *International Training and Outreach*, above.

[19] The Federal CIO Council was first established by Executive Order 13011 in 1996 and later codified by Congress in the E-Government Act of 2002. The CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. See the CIO Council website at *http://www.cio.gov/pages.cfm/page/About-Us.*

[20] *http://www.cio.gov/committees.cfm/csec/3/cid/6*

- **Development and Education Subcommittee** – DHS Privacy Office staff led Subcommittee efforts to present a two-hour workshop on *Privacy Training and Awareness Best Practices* which was attended by 120 staff from numerous Executive branch agencies. The workshop featured interactive sessions and methods for creating a culture of privacy in federal agencies. Office staff also supported the Subcommittee's creation of a new web portal to provide Privacy Committee member agencies with ready access to the catalogue of privacy education and awareness resources available in the federal community.
- **Federal Privacy Resources Web page** – DHS Privacy Office staff supported a Privacy Committee initiative to promote greater transparency in Federal Government activities by developing a new privacy resources page on the Federal CIO Council website.[21] The webpage features links to 55 Department and agency privacy homepages as well as available links to all associated PIAs and SORNs.

Other Interagency Initiatives.

- **National Strategy for Trusted Identities in Cyberspace (NSTIC)** – The NSTIC, issued in April 2011, advances a bold vision for enhancing both the privacy and security of online transactions by improving authentication and identity management in cyberspace. As one of the original federal agency contributors to this landmark document, the DHS Privacy Office continued to provide privacy subject-matter expertise to the Department of Commerce program office tasked with implementation of the strategy.[22]
- **National Science and Technology Council (NSTC)[23] Subcommittee on Privacy and Internet Policy, International Working Group** – DHS Privacy Office staff regularly contributes to the work of the NSTC Subcommittee on Privacy and Internet Policy International Working Group. The Working Group serves as an interagency forum for discussion on emerging international privacy issues, and is a valuable resource for staying apprised of international privacy engagement undertaken by the Federal Government. Office staff contributed to the Working Group's development of a United States Government response to the proposed European Union Data Protection Regulation and Directive.[24]
- **National Security Telecommunications Advisory Committee (NSTAC)[25] Nationwide Public Safety Broadband Network Scoping Committee** – DHS Privacy Office staff provides privacy subject-matter expertise to the NSTAC Nationwide Public Safety Broadband Network (NPSBN) Scoping Committee, which is responsible for developing recommendations for the implementation of the NPSBN.

[21] *http://www.cio.gov/modules/privacy/*

[22] *http://www.nist.gov/nstic/about-nstic.html*

[23] The National Science and Technology Council (NSTC) was established by Executive Order 12881 on November 23, 1993. This Cabinet-level Council is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise. *http://www.whitehouse.gov/administration/eop/ostp/nstc*

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

[25] *http://www.ncs.gov/nstac/*

Engaging the Public

Throughout this reporting period, the DHS Privacy Office continued to actively promote awareness and robust public dialogue on vital privacy issues. The Office developed, sponsored, and participated in events aimed at educating and engaging the federal workforce, the advocacy community, and the public on privacy-related topics, including:

- *DHS Privacy Office Speakers Series:* Led by PPAT, the Speakers Series, now in its fifth year, provides an opportunity to federal and private sector experts to engage in informal discussions with federal agency staff on privacy-related topics. During this reporting period, the Office hosted four events centering on the theme of online privacy and cybersecurity. Topics included:
  - *Are You Living with a Zombie? Botnets and Their Innocent Owners;*
  - *Nothing to Hide?* (theories of privacy for the information age);
  - *The Federal Government's Cybersecurity Program;* and
  - *Virtual Worlds, Privacy, and the Panopticon.*
- *Redesigned FOIA website:* The DHS FOIA website was reconfigured to maximize usability and now features a simplified menu and graphic links to rich content. The reorganized DHS online FOIA library—a key component of the site—brings together documents by type (such as directives, instructions, frequently requested records, etc.) and includes a link requesters can use to check the status of their FOIA requests. 19,897 pages were proactively posted during the reporting period, including some 600 pages of records pertaining to Occupy Wall Street, and 585 relating to Jones Act Waivers.
- *Quarterly privacy advocate meetings:* The Chief Privacy Officer continued to host a series of quarterly informational meetings with members of the advocacy community. The Chief Privacy Officer also updates the privacy advocacy community periodically by email or telephone conference calls about new relevant DHS reports or activities.
- *DHS Blog:* The Chief Privacy Officer contributed to the DHS Blog, highlighting how the DHS Privacy Office works to embed privacy protections into all DHS operations.
- *Speaking Engagements:* The DHS Chief Privacy Officer and DHS Privacy Office staff spoke on privacy topics at 20 events during this reporting period. Appendix E includes a list of these engagements.

DHS Privacy and Transparency Training

The DHS Privacy Office continued to execute its ongoing responsibility to ensure that DHS personnel understand the privacy implications of their daily work and handle information in accordance with the Privacy Act and DHS policy. To that end, the Office develops and provides a spectrum of privacy and transparency-related training for DHS personnel at every level.

Accomplishments and highlights from this reporting period include:

- *Updated mandatory annual privacy training:* In June 2012, the Office implemented a new mandatory online training course on DHS privacy practices which features interactive case studies to illustrate proper methods of safeguarding PII.
- *Issued a revised DHS Handbook for Safeguarding Sensitive Personally Identifiable Information*, which sets minimum standards for how Department personnel should handle Sensitive PII in paper and electronic form during their everyday work activities.
- *Cutting-edge FOIA training:* The Office hosted a series of topical trainings on evolving FOIA issues, including:
  - DOJ, Office of Information Policy (OIP) workshop on FOIA Exemptions 5, 6 and 7.
  - An OIP-led session on consultations, referrals, and interagency coordination; and
  - A specially-tailored version of the Office of Government Information Services' popular alternative dispute resolution workshop.
- *Annual Privacy Compliance Workshop:* In June 2012, over 200 personnel from multiple federal agencies attended the DHS Privacy Office Annual Privacy Compliance Workshop. This eight hour workshop provides in-depth training on DHS privacy compliance processes and best practices.
- *Privacy training for Chief Human Capital Officer staff (CHCO):* The DHS Privacy Office provided classroom training for all senior managers in CHCO on privacy compliance and best practices.
- *Privacy training for IT project managers:* Upon the request of the DHS CIO, the DHS Privacy Office provided classroom-based privacy compliance training tailored for IT project managers.

Reporting

Public reporting is an essential component of the DHS Privacy Office's efforts to further transparency of the Department's privacy-related activities and provide public accountability. The Office issues congressionally-mandated public reports that document progress in implementing DHS privacy and FOIA policy, including this report. During the reporting period, the Office issued the following reports. All of these reports, as well as those from prior years, can be accessed on our website at *www.dhs.gov/privacy*.

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

- *2011 Annual FOIA Report to the Attorney General of the United States (February 2012):*[26] This report provides a summary of Component-specific data on the number of FOIA requests received by the Department, the disposition of such requests, reasons for denial, appeals, response times, pending requests, processing costs, fees collected, and other statutorily required information;
- *2012 Chief Freedom of Information Act Officer Report to the Attorney General of the United States (March 2012):*[27] This report discusses actions taken by the Department to apply the presumption of openness and to ensure that DHS has an effective system for responding to requests, increases proactive disclosures, fully utilizes technology, reduces backlogs, and improves response times; and
- *2011 DHS Data Mining Report to Congress (February 2012):* This report describes DHS activities already deployed or under development that fall within the *Federal Agency Data Mining Reporting Act of 2007* [28] definition of data mining. It presents complete descriptions of the Automated Targeting System (ATS) Passenger and Land modules administered by CBP, and the Data Analysis and Research for Trade Transparency System, administered by U.S. Immigration and Customs Enforcement (ICE). The report describes three new uses of ATS by TSA, ICE, and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, respectively, in conjunction with CBP. The report also includes a brief summary of CBP's new Analytical Framework for Intelligence (AFI), which was then in development.[29]

The Chief Privacy Officer and DHS Privacy Office staff provide briefings to members of Congress on privacy and FOIA-related matters upon request. A complete list of briefings during this reporting period is provided in Appendix F.

[26] *http://www.dhs.gov/xlibrary/assets/privacy/privacy-foia-annual-report-fy-2011-dhs.pdf*
[27] *http://www.dhs.gov/xlibrary/assets/privacy/dhs-chief-foia-officer-report-2012.pdf*
[28] 42 U.S.C. § 2000ee-3
[29] None of these programs make decisions about individuals solely on the basis of data mining results. The DHS Privacy Office continues to monitor each of these programs to ensure that privacy protections are implemented. Should any other Department programs seek to engage in data mining in the future, the DHS Privacy Office will work with them to build in privacy by design and will describe their activities in future data mining reports.

Integrate

III. INTEGRATE Compliance

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

Privacy Compliance

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

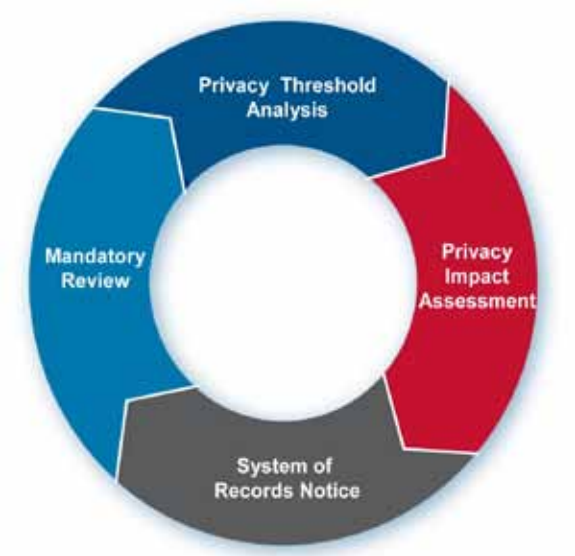


Figure 3: DHS Privacy Office Compliance Process

The DHS Privacy Office uses PIAs to establish guidelines based on the FIPPs for Department programs, systems, initiatives, and rulemakings. The Office is responsible for ensuring that the Department meets statutory requirements such as *Federal Information Security Management Act* of 2002 (FISMA)[30] privacy reporting. The Office also conducts privacy reviews of Office of Management and Budget (OMB) 300 budget submissions, and supports Component Privacy Officers and PPOCs to ensure that privacy compliance requirements are met.

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

[30] 44 U.S.C. § 3544.

- At the end of June 2011, the Department's FISMA privacy score showed that 77 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 95 percent of required SORNs had been completed. As of June 2012, the Department has improved this score to 82 percent of PIAs for required FISMA-related systems, and 95 percent of SORNs.[31]
- Issued a Directive and Instruction on Computer Matching Agreements (CMA) and formally established a DIB to oversee CMAs as required by the computer matching provisions of the Privacy Act. Under this Directive, the Chief Privacy Officer serves as the Chairperson of the DIB. This new Directive and Instruction provide clarity to the process for having a CMA approved by the Department to allow for sharing under a matching agreement, as required under 5 U.S.C. § 552a(o)-(u). During the reporting period, the Department approved seven CMAs with the SSA and with several state employment and health agencies. Additional information on the DHS DIB is included in Appendix C.
- Collaborated with the Chief Information Officer's Chief Information Security Officer (CISO) group to further embed privacy into the security authorization process. CISO updated its FISMA compliance tracking system to automatically invalidate PTAs older than 3 years, prompting system owners to review and resubmit PTAs as required by DHS privacy policy. This effort has improved the accuracy and completeness of information provided in the PTAs, which, as noted above, serve as the basis for the DHS Privacy Office's determination as to whether a PIA and/or SORN is required.
- Reviewed over 200 IT investments for compliance with privacy requirements as part of the annual OMB 300 budget review process. The DHS Privacy Office failed eight programs for their lack of privacy compliance documentation. The Office has actively worked with the eight programs to bring them into compliance and anticipates that several will pass during the review process that begins in June 2012.

The DHS Privacy Office completed the reporting period with a Department-wide Federal Information Security Management Act privacy score of 95 percent for SORNs and 82 percent for required IT system PIAs.

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

The DHS Privacy Office publishes new and updated PIAs on its website at www.dhs.gov/privacy. During the reporting period, the Chief Privacy Officer approved 76 new or updated PIAs. Figure 4 illustrates the number of approved PIAs completed by Component during this reporting period.[32]

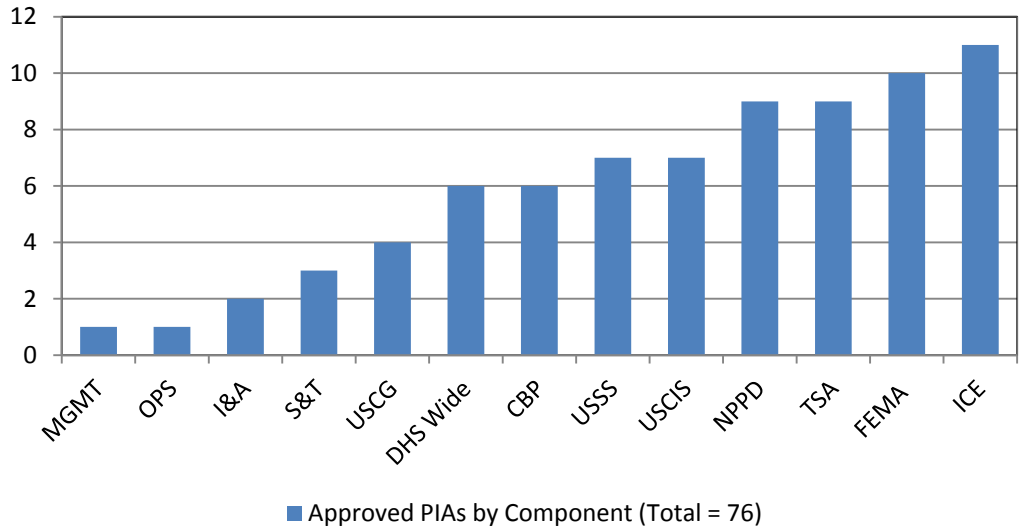


Figure 4: Number of Approved PIAs by Component During the Reporting Period

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

- **DHS/ALL/PIA-041 One DHS Overstay Vetting Pilot**. DHS conducted the One DHS Overstay Vetting Pilot to improve DHS's ability to identify and vet foreign nationals who have remained in the United States beyond their authorized period of admission (overstays). The pilot identified ways to streamline data sharing between NPPD's US-VISIT, CBP, and ICE. CBP, ICE, and US-VISIT worked with the DHS Privacy Office to complete a PIA specific to the Overstay Vetting Pilot to add another layer of analysis and transparency. Data sharing conducted through this pilot allows DHS to better identify overstays, and to determine which overstays are the highest law enforcement or national security priority for enforcement action by ICE.

[32] This represents the total number of new or updated PIAs that were approved by the Chief Privacy Officer during the reporting period. Appendix D provides a list of approved PIAs that were published during the reporting period. A number of PIAs were approved, but not published, during the reporting period. This may occur for two different reasons: (1) the PIA was deemed to contain sensitive information (such as Law Enforcement Sensitive or otherwise classified material) and accordingly the entire document or selected portions were withheld from publication; or (2) publication of the PIA was delayed for administrative reasons. Information relating to PIAs approved but not published during the reporting period due to sensitive or classified content is being provided to Congress in a separate annex to this report. Approved PIAs published after June 30, 2012, will be included in the DHS Privacy Office 2013 Annual Report, and made available at *www.dhs.gov/privacy.*

- **DHS/TSA/PIA-018(e) Secure Flight Program Update.** The TSA Secure Flight program screens aviation passengers and certain non-travelers before they access airport sterile areas or board aircraft. This screening compares these individuals to the No Fly and Selectee portions of the consolidated and integrated terrorist watch list and to other watch lists maintained by the Federal Government when warranted by security considerations, and against a list of passengers with redress numbers, i.e., passengers who have been assigned a unique number by the DHS Traveler Redress Inquiry Program (DHS TRIP). In August 2011, TSA updated the Secure Flight PIA to reflect a number of changes, including: (1) the initiation of a Known Traveler proof of concept starting with individuals enrolled within CBP Trusted Traveler programs, and expected to expand to include other populations such as members of the military and transportation sector workers receiving TSA security threat assessments; and (2) the receipt by Secure Flight of aircraft operator frequent flyer status codes for use in conjunction with risk-based security rules using Secure Flight Passenger Data.

  The PIA update reflected the transition from proof of concept to operational program of the Known Traveler and frequent flyer concepts within a program known as TSA Pre✓™. In addition, TSA will create, maintain, and screen against a watch list of individuals who, based upon their involvement in violations of security regulations of sufficient severity or frequency, are disqualified from receiving expedited screening for a fixed period of time or permanently.
- **DHS/CBP/PIA-006(b) ATS Update.** As a decision support tool operated by CBP, ATS compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. ATS assists CBP officials in identifying individuals and cargo entering and departing the United States that need additional review. Because CBP expanded the modules in ATS, and expanded the datasets ATS uses and stores, CBP published the PIA and SORN to notify the public of the changes, to describe the potential privacy risks, and to identify the safeguards that mitigate those risks.

- **DHS/ICE/PIA-032 FALCON[33] Search & Analysis System (FALCON-SA).** ICE established a consolidated information management system called FALCON-SA. This system enables ICE law enforcement and homeland security personnel to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal and administrative laws. ICE agents, criminal research specialists, and intelligence analysts use FALCON-SA to conduct research that supports the production of law enforcement intelligence products. In addition, FALCON-SA provides lead information for investigative inquiry and follow-up, assists in the conduct of ICE criminal and administrative investigations, assists in the disruption of terrorist or other criminal activity, and discovers previously unknown connections among existing ICE investigations. ICE's use of the system is always predicated on homeland security, law enforcement, and intelligence activities. FALCON-SA is an internal system used only by ICE.

  In order to mitigate privacy and security risks associated with the deployment of FALCON-SA, ICE has built technical safeguards into the system and developed a governance process that includes the operational components of ICE Homeland Security Investigations, the oversight functions of the ICE Privacy Office, the Office of the Principal Legal Advisor, and the ICE Office of the Chief Information Officer.

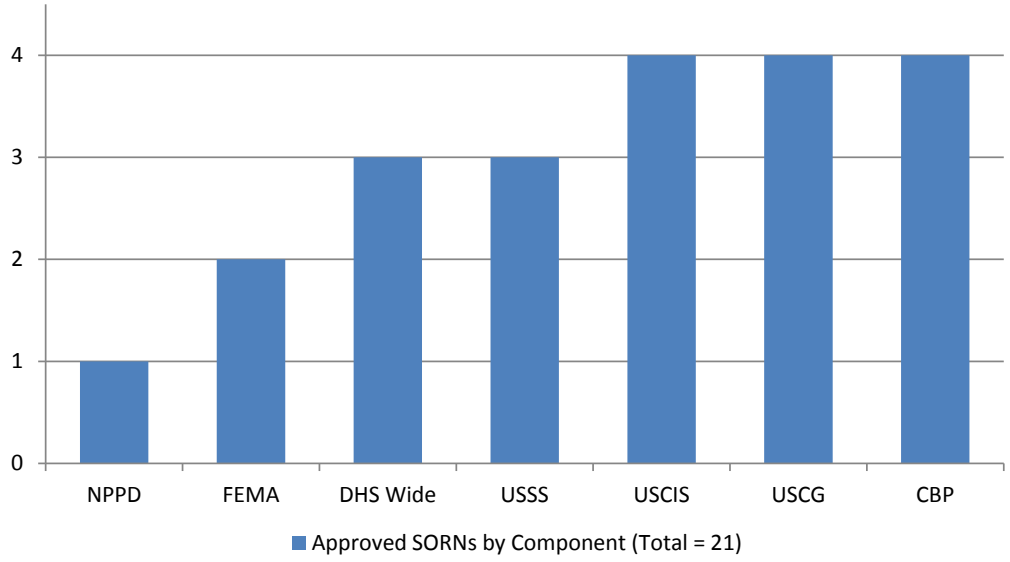


Figure 5: Number of Approved SORNs by Component During the Reporting Period

During the reporting period, the Chief Privacy Officer approved and published 21 SORNs which are listed by Component in Appendix D. Figure 5 illustrates the number of SORNs completed by Component during this reporting period.

[33] FALCON is the name of the system. It is not an acronym.

Intelligence Product Reviews

The DHS Privacy Office reviews DHS I&A classified and unclassified briefings, products, reports, directives, and other materials for privacy-related issues, and for compliance with privacy laws and regulations before release to the intelligence community and state and local stakeholders. DHS Privacy Office staff apply the FIPPs, pertinent executive orders, and DHS Directives during the review process. Staff also participate in the key working groups led by I&A on terrorism-related issues.

During this reporting period, DHS Privacy Office staff reviewed approximately 176 intelligence products and 421 Intelligence Information Reports (IIRs).[34] The Office clears approximately 90 percent of all IIRs and products on first review with only minimal correction—a significant improvement from last year's 80 percent for IIRs and 73 percent for products. The Office's review of IIRs and intelligence products continues to strengthen the quality of the products. Further, improvements to the IIR and product clearance rates demonstrate an enhanced integration of privacy protections.

DHS Privacy Office staff provided several briefings to I&A staff about protecting privacy when writing reports and also participated as instructors in I&A's Reports Officers Basic Course (ROBC). The DHS Privacy Office also worked with I&A to develop expanded privacy-related course materials for a new course that will replace the ROBC, and will conduct the privacy portion of the new training class in an interactive, classroom setting.

FOIA Compliance

In addition to the DHS Privacy Office's daily business of processing FOIA requests and appeals (909 FOIA requests received, and 895 processed, during the reporting period), significant progress was made during this reporting period to integrate FOIA compliance into Department operations. Specifically, the Office took steps to standardize the FOIA process and ensure excellence across the Department by piloting an electronic FOIA solution for enterprise deployment. Currently, FOIA tracking and reporting data resides throughout the Department in several databases with limited interoperability. The comprehensive application selected enables requests and appeals to be entered into the system from written or electronic requests. Options for printing or emailing acknowledgements and standard responses, along with other authorized correspondence, are included and fees can be calculated based on agency policy. The new software program also includes an advanced electronic redaction toolset for search, retrieval, and redaction. The Office expects that the implementation of the electronic solution will increase FOIA processing efficiencies and improve data integrity.

[34] IIRs 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.

The DHS Privacy Office also worked to develop best practices to manage the Department's backlog of FOIA requests. By meeting with Component FOIA Officers and FOIA officials from other federal agencies, Office staff gained insight into how technology, training, and staff development can converge to reduce the backlog, particularly through day-to-day case management. Beginning in June 2012, the Office deployed specialists to the Components to help them achieve processing efficiencies and reduce their FOIA backlog.

More detailed information concerning FOIA operations can be found in the 2012 *Chief Freedom of Information Act Officer Report to the Attorney General of the United States*, at *www.dhs.gov/privacy*.

Implement

IV. IMPLEMENT Privacy Oversight

The DHS Privacy Office established its new Privacy Oversight Team in February 2012, as an outgrowth of the Office's 2012–2015 Strategic Plan. The Privacy Oversight Team includes several pre-existing Office functions that logically follow from the Office's core responsibility to ensure that Department programs and systems comply with DHS privacy policy: Privacy Compliance Reviews (PCR), privacy investigations, privacy incident response, and privacy complaint handling and redress. The Privacy Oversight Team is still a new team, but the synergies created by bringing together these complementary functions are already strengthening the Office's oversight role throughout DHS.

Privacy Compliance Reviews

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

PCRs may result in recommendations to a program, updates to privacy documentation, informal discussions on lessons learned, or a formal internal or publicly available report. During this reporting period, the DHS Privacy Office expanded its use of PCRs at DHS, completing five public PCR reports. These PCRs covered a range of programs including cybersecurity (EINSTEIN Program), information sharing (Immigration and Customs Enforcement Pattern Analysis and Information Collection (ICEPIC) Law Enforcement Information Sharing Service (LEIS)), and the Department's use of social media (National Operations Center Publicly Available Media Monitoring and Situational Awareness Initiative; DHS Use of Social Networking Interactions and Applications Communications/Outreach/Public Dialogue, and DHS Use of Unidirectional Social Media Applications Communications and Outreach).[35]

The PCR's positive influence is evident in the development of a framework to aid the DHS Privacy Office in evaluating and remedying privacy compliance gaps. The PCR report on the ICEPIC LEIS Service, referenced above, included a recommendation for adopting such a framework. The framework, developed by Office staff in collaboration with the DHS Component Privacy Officers, identifies four factors to consider before identifying a remedy for a compliance gap, including (1) the nature and severity of the gap; (2) the privacy impact; (3) any mitigating factors; and (4) the mission criticality of the system or program affected by the gap. The framework also identifies possible remedies for closing compliance gaps, and will be used across all of the Office's functions. To encourage heightened awareness and attention to privacy requirements, the Chief Privacy Officer distributed the framework to DHS and Component leadership in June 2012.

The DHS Privacy Office staff leads an ongoing PCR of DHS Component participation in the DHS Information Sharing Environment Suspicious Activity Reporting (ISE-SAR) Initiative.[36] To date, Office staff has reviewed ISE-SAR contributions to the Nationwide Suspicious Activity Reporting Initiative Shared Space by the NPPD/National Infrastructure Coordination Center, NPPD/Federal Protective Service, TSA/Federal Air Marshals, and the United States Coast Guard.

[35] These PCR reports are available on the Privacy Office's website under "Privacy Investigations and Compliance Reviews" *(http://www.dhs.gov/files/publications/gc_1284657535855.shtm).*

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

DHS is still in the early stages of implementing this initiative, and the PCR provides a unique opportunity to identify potential areas for improvement.

The Privacy Oversight Team works closely with colleagues throughout the DHS Privacy Office to identify high-risk, high profile programs that would benefit from a PCR. Increasingly, a PCR requirement is being included in Department PIAs. As the PCR process becomes more embedded at DHS, we expect PCRs to become an increasingly valuable tool for both the Office and the programs undergoing review. In addition, the Office provides guidance on conducting PCRs to other federal agencies in an effort to foster adoption of the PCR process throughout the federal privacy community.

In a process similar to a PCR, the DHS Privacy Office also oversaw implementation of ATS (see description in Section III) and several DHS information sharing agreements with the NCTC. The DHS Chief Privacy Officer, together with representatives of CRCL, OGC, and relevant program staff, conduct quarterly reviews of these activities to assess whether privacy and civil liberties protections are adequate and consistently implemented.

Investigations

During this reporting period, the DHS Privacy Office conducted two investigations that led to findings of non-compliance with DHS privacy policy.[37] One of these investigations involved a Component's use of social media for operational purposes without appropriate oversight or protections for the collection and use of PII. Based on its findings, the DHS Privacy Office provided the Component a set of recommendations that then formed the basis for the Department-wide Directive, *Privacy Policy for Operational Use of Social Media*. The Office, and, in particular, the new Privacy Oversight Team, was instrumental in developing this Directive, which is discussed more fully in Section I of this report.

The second investigation was prompted by a referral from the DHS Office of Inspector General. The purpose of the investigation was to determine whether a DHS Component's information sharing pilot with an external agency was in compliance with DHS privacy and information sharing policy and the Privacy Act. The investigation resulted in a letter from the Chief Privacy Officer to the Deputy Secretary of Homeland Security detailing the conclusions drawn from the investigation and steps to be taken to ensure that any future pilot is implemented in a privacy-protective manner.

The DHS Privacy Office expanded its use of Privacy Compliance Reviews this year, completing five public reports covering a range of programs including cybersecurity, information sharing, and the Department's use of social media.

[37] Congress expanded the authorities and responsibilities of the Chief Privacy Officer in 2007 in Section 802 of the 9/11 Commission Act, which added investigative authority, the power to issue subpoenas to non-federal entities, and the ability to administer oaths, affirmations, or affidavits necessary to investigate or report on matters relating to responsibilities under Section 222 of the Homeland Security Act. 6 U.S.C. § 142.

Privacy Incident Handling

The DHS Privacy Office manages privacy incident response for the Department. Office staff works to ensure that all privacy incidents are properly reported, investigated, mitigated, and remediated as appropriate, in collaboration with the DHS Security Operations Center (SOC), Component Privacy Officers and PPOCs, and DHS management. During this reporting period the Office revised and reissued the *DHS Privacy Incident Handling Guidance* (PIHG),[38] the foundation of privacy incident response in the Department, to streamline the guidance provided and incorporate lessons learned since 2007, when the PIHG was first published.

During this reporting period, 683 privacy incidents were reported to the DHS SOC, an increase of 34 percent from the last reporting period.[39] The Department investigated, mitigated and closed 598 (88 percent) of those privacy incidents. Figure 6 shows the number (and percent of total) of reported DHS privacy incidents by type of incident. Figure 7 shows the number (and percent of total) of reported DHS privacy incidents by Component.

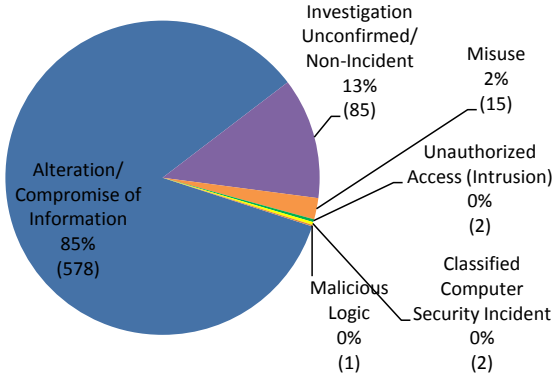


Figure 6: Percentage and Number of DHS Privacy Incidents by Type July 1, 2011- June 30, 2012 (total = 683)[40]

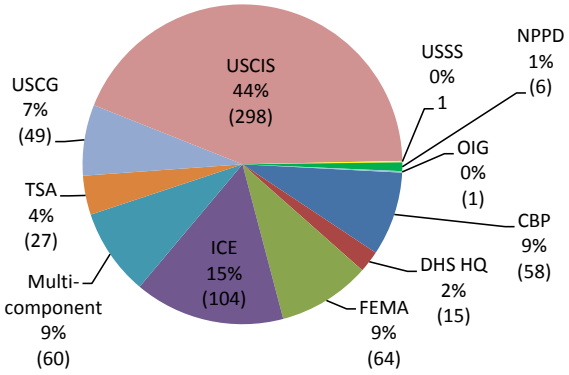


Figure 7: Percentage and Number of DHS Privacy Incidents by Component July 1, 2011- June 30, 2012 (total = 683)[41]

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

[39] The increase in the number of incidents is attributable in part to increased reporting of suspected privacy incidents as a result of training provided by the DHS Privacy Office.

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

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

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

- Hosting the third annual DHS Core Management Group Meeting in September 2011, during which stakeholders met with the Chief Privacy Officer to discuss privacy incidents and incident handling procedures;
- Holding Privacy Incident Handling Quarterly Meetings in August 2011 and January and May 2012, providing an opportunity for Component Privacy Officers, PPOCs, and DHS SOC managers to share best practices and provide feedback on privacy incident management, mitigation, and prevention;
- Conducting site visits and meetings with DHS Components, to discuss their privacy incident handling procedures and recommendations for improvement; and
- Providing guidance on privacy incident handling to staff of the National Institutes of Health and the Department of Defense.

Privacy Complaint Handling and Redress

The DHS Privacy Office is responsible for ensuring that the Department has procedures in place to receive, investigate, respond to, and provide redress for complaints from individuals who allege privacy or privacy compliance violations by the Department. U.S. citizens, Legal Permanent Residents, visitors to the United States, and aliens may submit privacy complaints to the Department.[42] The Privacy Oversight team also reviews and responds to privacy complaints referred by employees throughout the Department or submitted by other government agencies, the private sector, or the general public. DHS Components manage and customize their privacy complaint handling processes to align with their specific missions and to comply with Department complaint handling and reporting requirements. Between June 1, 2011 and May 31, 2012, the Department received 1,192 privacy complaints.

Section 803 of the 9/11 Commission Act and OMB Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*[43] require that the Department report quarterly to Congress on privacy complaints received and their disposition. Section II of this report includes additional information on the DHS Privacy Office's public reporting responsibilities.

Figure 8 shows the categories and disposition of privacy complaints the Department received between June 1, 2011 and May 31, 2012.[44]

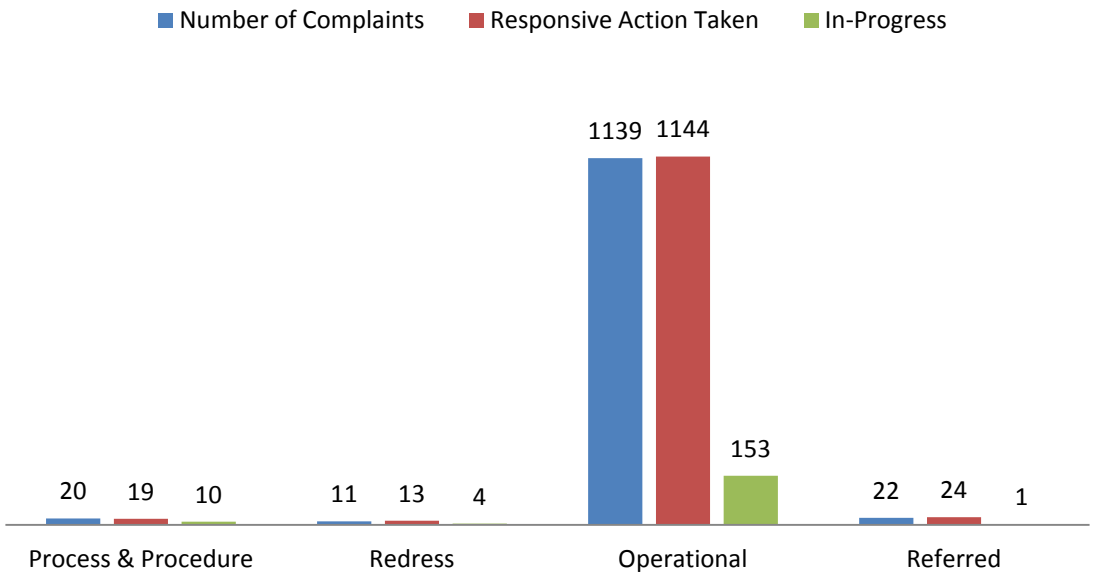


Figure 8: Privacy Complaints Received by DHS June 1, 2011 - May 31, 2012 [45]

[42] The Department accepts complaints pursuant to the DHS Mixed System Policy set out in DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons, available at *http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.* The Mixed Systems Policy is discussed in Section II.B of the DHS Privacy Office's 2011 Annual Report to Congress, available at *http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacy_rpt_annual_2011.pdf.*

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

[44] The quarterly reporting period from June 2012 through August 2012 was ongoing at the close of the reporting period for this Annual Report. Statistics on privacy complaints submitted before June 2011 are provided in the DHS Privacy Office's Section 803 Reports, available at *http://www.dhs.gov/files/publications/editorial_0514.shtm.*

[45] The totals represented include complaints from previous periods that have not yet been resolved. The categories of complaints are defined in OMB M-08-21 and included in the DHS Privacy Office's Section 803 Reports.

Illustrative examples of privacy complaints submitted to the Department are included in the DHS Privacy Office's Section 803 Reports.[46]

Privacy Act Amendment Requests

Under section (d)(2) of the Privacy Act, an individual may submit a request to the Department seeking amendment of his or her own records.[47] As required by *DHS Privacy Policy Guidance Memorandum 2011-01, Privacy Act Amendment Requests*, Component Privacy Officers and FOIA Officers are responsible for tracking all Privacy Act Amendment requests and reporting the disposition of those requests to the DHS Privacy Office.[48] The Privacy Oversight Team serves as the repository for those statistics. During the reporting period the Office received two Privacy Act Amendment requests and DHS Components received an additional 49 requests. Figure 9 shows Privacy Act Amendment Requests received by DHS during the reporting period by Component and disposition.

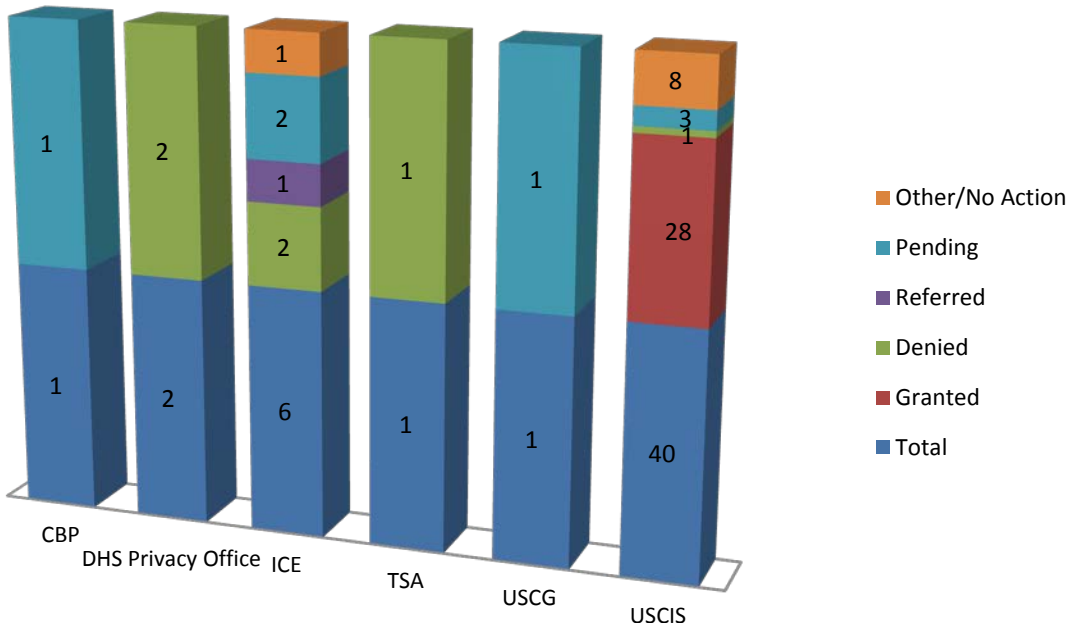


Figure 9: Privacy Act Amendment Requests by Component and Disposition July 1, 2011-June 30, 2012

[46] Available at *http://www.dhs.gov/files/publications/editorial_0514.shtm.*
[47] 5 U.S.C. § 552a (d)(2).
[48] *http://www.dhs.gov/xlibrary/assets/privacy/privacy-policy-guidance-memorandum-2011-01.pdf*

Non-Privacy Act Redress Programs

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

- *DHS TRIP.* Now in its fifth year of operation, 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.[49] The Chief Privacy Officer is a member of the DHS TRIP Advisory Board. To date, DHS TRIP has received more than 155,000 requests for redress and has an average response time (from the time of first submission to final resolution) of approximately 111 days. DHS TRIP has been focused on closing older cases, which directly impacts the average processing time. In addition:
  - DHS reduced cases open for more than 180 days by over 85 percent from last year.
  - Redress inquiries alleging non-compliance with DHS privacy policy are reviewed by the DHS Privacy Office Oversight Team and are either referred to the relevant Component or are handled by the Office, as appropriate.
- *NPPD/US-VISIT Redress Program.* US-VISIT collects and maintains biometric information obtained in support of DHS missions. One of the main goals of the US-VISIT redress program is to maintain and protect the integrity, accuracy, privacy, and security of the information in its systems. US-VISIT responded to 1,352 redress requests during the reporting period.
- *Transportation Sector Threat Assessment and Credentialing Redress.* TSA's Office of Law Enforcement/ Federal Air Marshal Service (OLE/FAMS) conducts security threat assessments and completes adjudication services in support of TSA's mission to protect U.S. transportation systems from individuals who may pose a threat to transportation security. OLE/FAMS provides daily checks on over 12 million transportation sector workers against federal watch lists. OLE/FAMS provides a redress process that includes both appeals and waivers for transportation sector workers who feel that they were wrongly identified as individuals who pose a threat to transportation security. Typical redress requests have involved documentation missing from initial submissions, immigration issues, or requests for waivers of criminal histories. During the reporting period, OLE/FAMS granted 9,517 appeals and denied 306. Additionally, OLE/FAMS granted 2,994 waivers and denied 680.

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

Inspire

V. INSPIRE Workforce Excellence

The 2012 strategic planning process, discussed in the Background Section, identified a new strategic goal focused exclusively on the DHS Privacy Office workforce. As a recognized leader in the federal privacy community, it is only fitting that the Office devotes a strategic goal to developing the individuals who make up this unique organization. The FY 2012–2015 Strategic Plan sets a high standard for the Office's workforce, aiming to "develop the best privacy and disclosure professionals in the Federal Government." This year, the Office worked diligently to make efficient use of its existing resources and maintain its leadership role in the federal privacy community through workforce development efforts. In addition to the strategic organizational realignment, which reflects that of a mature privacy organization, the Office instituted detail and rotational assignments designed to inspire excellence in its workforce.

Workforce Development Activities

In an effort to inspire excellence in our employees and provide new opportunities, the DHS Privacy Office implemented the DHS Privacy Office Internal Rotational Assignment Program. This program provides specialized skills as well as leadership development opportunities for employees. Skill development experiences are lateral moves within the Office that broaden employees' technical knowledge base and provide exposure to different responsibilities and functions. Leadership experiences involve increased team management roles that prepare employees for progressively higher levels of responsibility. These internal rotational assignments provide valuable skill development and "on the job" training for Office personnel at no additional cost to the organization.

The DHS Privacy Office also provided tailored support to NPPD, CBP, ICE, the Office of the Inspector General (OIG), and the Department of Commerce through rotational assignments of Office personnel to these entities. Office staff participated in these temporary rotational assignments in order to:

- maintain and coordinate operational processes for privacy compliance documentation;
- process backlogged FOIA and Privacy Act requests within established deadlines;
- coordinate international activities, strategic priorities, and policy objectives; and
- work directly with operations personnel domestically and abroad to coordinate U.S. and foreign government activities.

Such rotational opportunities also provide professional growth and skill development opportunities for Office personnel while furthering the DHS Privacy Office mission of ensuring privacy protections and disclosure policies are fully implemented in all DHS programs.

Further, the Office sponsored three professional development workshops for staff during the reporting period. These workshops focused on the DHS Performance Management Core Competencies of Leadership, Communication, and Teamwork/Cooperation, and provided practical lessons on leadership styles, active listening, best practices for briefing and facilitation, how to develop and maintain collaborative working relationships, and strategies for enhancing teamwork. With the assistance of the DHS Chief Human Capital Officer, these workshops featured managers and experts from throughout DHS and other federal agencies.

As a result, the Office was able to provide this valuable training to the entire staff with considerable cost-savings over comparable workshops offered by outside vendors.

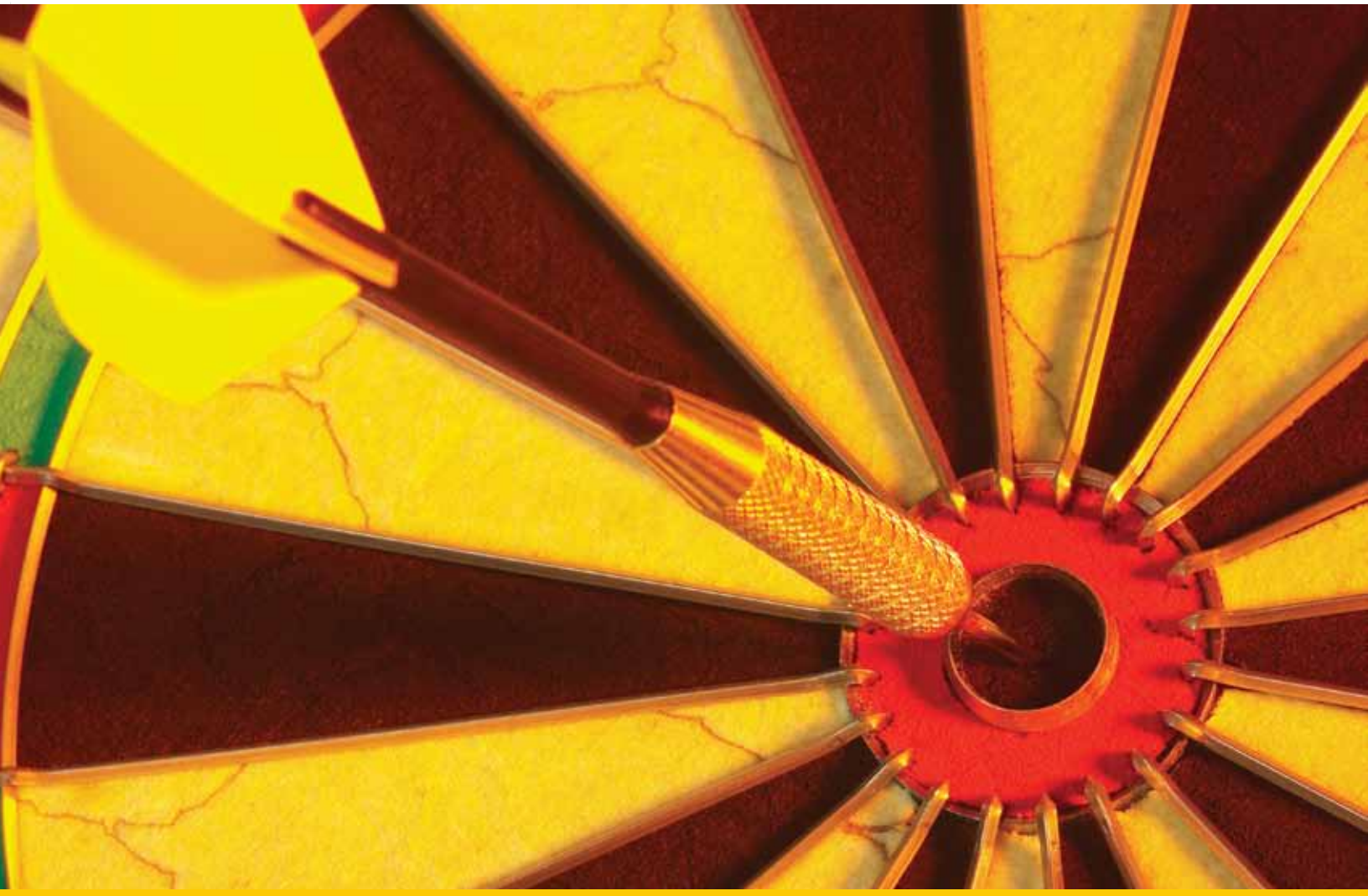
During this reporting period, the DHS Privacy Office also created an Employee Training Resource Center on the internal DHS intranet site. This resource provides information to Office staff on detail/rotational opportunities, training and education, and leadership development opportunities.

Office Sustainment and Efficiency

To further support its staff's work, the DHS Privacy Office has continued to work diligently to contain costs and identify savings wherever possible. During the reporting period, the office has focused on sustainable and efficient use of resources, such as expanding opportunities for in-house or no-fee training, minimizing reliance on contractor support, and reducing costs associated with office space. In May 2012, the Office completed plans to reduce office space by relocating to a DHS shared facility. Through improved efficiency, management of technology, reduced physical space requirements, and better leveraging of internal resources, the Office has sustained its long-term ability to carry out its mission.

The DHS Privacy Office implemented an Internal Rotational Assignment Program to provide specialized skills as well as leadership development opportunities for its staff at no additional cost.

This page intentionally left blank.



Impact

VI. IMPACT Component Privacy Programs and Operations

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

Federal Emergency Management Agency (FEMA)

The mission of the FEMA Privacy Office is to sustain privacy protections and minimize privacy impacts on FEMA's constituents, while supporting the agency in achieving its mission.

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

FEMA Privacy Policy Leadership and Development

- Named a new Privacy Officer to lead FEMA's effort to create a culture of privacy awareness and compliance throughout the Agency. The FEMA Privacy Officer updated the mission statement and established a new vision with attendant program objectives.
- Furthered and completed the FEMA Administrator's initiative to "Decrease Agency Vulnerability to Identity Theft," which entailed establishing a baseline inventory of FEMA IT systems and forms that collect or maintain Social Security numbers (SSNs) and conducting a comprehensive review of each IT system and form to ensure SSNs are collected and maintained only when and where necessary and legally authorized. FEMA achieved a 22.6 percent reduction in the number of IT systems and forms collecting SSNs.

- Integrated privacy representation into FEMA's Policy Working Group to ensure that all polices are developed with privacy interests considered and to minimize the impact on individual privacy by necessary modifications.

FEMA Privacy Compliance

- Increased its FISMA score for SORNs from 98 percent to 100 percent during this reporting period. The FEMA FISMA score for PIAs similarly increased from 79 percent to 100 percent.
- Completed or updated 103 PTAs, 10 PIAs, and 2 SORNs during the reporting period.
- Initiated a FISMA privacy compliance effort to bring all FEMA systems into compliance with privacy laws and related OMB, DHS, and FEMA privacy policies and guidance. This effort resulted in FEMA's achievement of a 100 percent FISMA score for both SORNs and PIAs.
- Renewed its June 2010 CMA with the U.S. Small Business Administration (SBA) to ensure that applicants for SBA Disaster Loans and DHS/FEMA Other Needs Assistance will not receive duplicate benefits for the same disaster. With the extension of the original CMA, FEMA and SBA will continue to share data under this CMA until February 2013.

FEMA Privacy Incident Response and Mitigation

- Continued efforts to increase privacy awareness and reduce privacy incidents through a comprehensive risk mitigation strategy, which includes:
  - policy regarding the proper email transmission of PII;
  - full deployment of laptops with encryption software;
  - initiative to decrease agency vulnerability to identity theft by reducing the number of systems and forms collecting SSNs;
  - privacy awareness training and education efforts; and
  - pro-active privacy risk analyses, site inspections, and compliance reviews.

FEMA Privacy Training and Outreach

- Revamped its mandatory annual privacy awareness training module and implemented it as both an instructor-led and on-line independent study course.
- Continued to conduct initial privacy awareness training on a weekly basis to all newly hired FEMA employees and contractors in the National Capital Region.
- Continued outreach efforts by facilitating specialized privacy awareness training webinars for FEMA personnel in Region IV, which includes Georgia, Mississippi, Alabama, Tennessee, Kentucky, and Florida.
- Hosted a two-day Privacy Compliance Foundations training for IT security professionals, program and project management professionals, system managers, and other personnel who handle or who are responsible for ensuring that electronic systems are in compliance with the privacy legal framework.

FEMA Privacy Oversight

In January 2012, the OIG initiated an audit of FEMA's privacy stewardship in field locations to evaluate the culture of privacy awareness at FEMA and determine if the agency is complying with the Privacy Act, E-Government Act, FISMA, Homeland Security Act, Executive Orders, OMB Privacy Guidance, privacy regulations, and DHS and FEMA privacy policies. The OIG review is ongoing.

National Protection and Programs Directorate (NPPD)

The mission of NPPD is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure.

During the reporting period, NPPD privacy staff (NPPD Privacy) engaged in the following activities to promote and protect privacy while supporting critical mission operations:

NPPD Privacy Policy Leadership and Development

- Developed a Management Directive on Privacy Protection Roles and Responsibilities to formalize Directorate privacy processes.
- Established a Social Media Working Group to evaluate existing or planned uses of social media and ensure compliance with privacy requirements.

NPPD Privacy Compliance

- Maintained its 100 percent FISMA score for both PIAs and SORNs during the reporting period.
- Completed or updated 31 PTAs, 8 PIAs, and one SORN during the reporting period.
- Conducted PIAs for several critical NPPD programs and systems, including:
  - **Joint Cybersecurity Services Pilot.** This voluntary information sharing program seeks to protect critical infrastructure information systems and networks.
  - **Dispatch and Incident Record Management Systems.** These systems enhance the sharing of law enforcement information collected through field interview reports.
  - **Ammonium Nitrate-Security Program.** This program seeks to provide systematic regulation, inspection, and enforcement of ammonium nitrate security standards.
  - **Critical Infrastructure Private Sector Clearance Program.** This program enables NPPD to sponsor designated private sector individuals for security clearances.
  - **Protected Critical Infrastructure Information (PCII) Program.** This program enables the private sector to authorize PCII users, and to submit and manage information designated as PCII.
  - **Linking Encrypted Network System.** This system enables authorized users to obtain, post, and exchange information through online portals.
  - **NPPD National Infrastructure Coordinating Center (NICC) Suspicious Activity Reporting (SAR) Initiative.** A new PIA and updated SORN were approved to clarify that redacted NICC reports are scrubbed of PII and identifying information relating to businesses.
  - **Biometric Interoperability between the U.S. Department of Homeland Security and the U.S. Department of Justice.** This PIA was updated to cover the expansion of biometric interoperability between DHS and the DOJ, including new users and a more comprehensive IDENT response.

- Reviewed over 20 information collections, including forms, surveys, and *Paperwork Reduction Act* (PRA) packages, to ensure proper collection of PII. As necessary, NPPD also wrote Privacy Act Statements and Privacy Notices to provide notice to individuals regarding the collection of their personal information.

- Created an inventory to manage Directorate information sharing agreements, and to ensure new information sharing agreements with federal, international, and state and local partners contain the necessary provisions to protect privacy.

NPPD Privacy Incident Response and Mitigation

- Provided role-based training to individuals involved in privacy incidents.
- Developed NPPD fact sheets providing best practices for protecting Sensitive PII while teleworking and sending email.
- Distributed business-card size privacy incident guides to Directorate personnel.
- Integrated *DHS Privacy Incident Handling Guide* procedures into Directorate roles and operations.
- Completed an Incident Response Plan that provides guidance to US-VISIT employees and contractors on the process that they need to follow in the case of an incident involving the unauthorized disclosure of PII.

NPPD Privacy Training and Outreach

- Developed and deployed a pilot to offer NPPD privacy training on the Homeland Security Information Network (HSIN) Connect Portal.
- Provided instructor-led privacy training for new employees at orientation, individuals with specific role-based privacy compliance requirements, and privacy stakeholders such as FOIA and PRA professionals.
- Launched the quarterly *NPPD Privacy Update*, and published privacy tips in internal communications to highlight emerging privacy issues that impact the NPPD mission, as well as issues pertinent to employees' personal privacy.
- Conducted the first joint NPPD-US-VISIT Annual Privacy Week, which drew over 300 participants from across NPPD, and earned both offices a "One NPPD Award" from the NPPD Under Secretary, which recognizes employees who represent the Department's leadership vision of "one DHS".

NPPD Privacy Oversight

- Participated in a PCR for the EINSTEIN Program, which concluded that NPPD was generally compliant with the requirements outlined in the EINSTEIN 2 PIA and Initiative 3 Exercise PIA, and fully compliant on collection of PII, use of PII, internal sharing and external sharing with federal agencies, and accountability requirements.

Office of Intelligence and Analysis (I&A)

I&A is one of two DHS Components that serve as elements of the nation's intelligence community. I&A is tasked to provide the homeland security enterprise with the intelligence and information it needs to keep the homeland safe, secure, and resilient. I&A provides intelligence support across the full range of DHS's missions to Department leaders, Components, state, local, tribal, and territorial governments, and the private sector. I&A ensures that information related to homeland security threats is collected, analyzed, and disseminated to all relevant stakeholders.

During the reporting period, the I&A Privacy Office (I&A Privacy) engaged in the following activities to promote and protect privacy while supporting the work of I&A:

I&A Privacy Policy Leadership and Development

- Focused on developing privacy guidance, assessing I&A directorates to identify gaps, and mitigating risks with regards to privacy.
- Issued a directive, *I&A Handling of Sensitive Personally Identifiable Information*, which provides I&A staff with a comprehensive process and requirements for the appropriate handling of Sensitive PII and establishes additional Sensitive PII training requirements and supervisory responsibilities.

I&A Privacy Compliance

- Completed or updated 23 PTAs, 2 PIAs, and zero SORNs during the reporting period.[50]
- The I&A Privacy Officer continually met with program managers assigned to develop or purchase information technology or information systems in order to review and identify any potential privacy impact.

I&A Privacy Incident Response and Mitigation

- Reported one privacy incident in which an employee improperly forwarded Sensitive PII to his private email address. to facilitate working at home. After an investigation, the employee deleted the file from his home computer and completed additional training on the proper handling of Sensitive PII to prevent further privacy issues.

I&A Privacy Training and Outreach

- Provided privacy training to new I&A employees each month.

[50] I&A, as an element of the intelligence community, is exempt from FISMA reporting requirements.

Science and Technology Directorate (S&T)

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

During the reporting period, the S&T Privacy Office (S&T Privacy) engaged in the following activities to promote and protect privacy while supporting the work of S&T:

S&T Privacy Policy Leadership and Development

- Coordinated with United States Citizenship and Immigration Services (USCIS) and the DHS Privacy Office to develop policies regarding the collection and use of DNA to support DHS operations, including a planned pilot of the Rapid DNA System (not yet operational). The pilot is intended to test a more efficient and cost-effective method of analyzing DNA for family relationship verification.
- Coordinated with CBP and NPPD to develop policies and compliance documentation for the Department's use of biometrics, including iris images.

S&T Privacy Compliance

- Achieved a FISMA score of 85 percent for PIAs and 100 percent for SORNs during this reporting period.
- Completed or updated 32 PTAs, 3 PIAs, and zero SORNs during the reporting period.
- Published a risk analysis on the Protected Repository for the Defense of Infrastructure Against Cyber Threats program, a clearinghouse that enables the sharing of selected data sets of internet traffic with approved researchers.
- Retired the SAFETY Act SORN and consolidated its content into Department-wide documentation (DHS/ALL-002 Mailing and Other Lists SORN).

S&T Privacy Incident Response and Mitigation

- Coordinated with the incident response team in the S&T Office of the Chief Information Officer to respond to a potential privacy incident involving the transmission of Sensitive PII. Upon further investigation, S&T Privacy determined that all recipients of the information had an authorized need to know the information and, therefore, closed the incident.
- Addressed the S&T Office of the Director of Operational Test and Evaluation program manager's privacy concerns regarding a malicious data breach of the Defense Acquisition University database that involved DHS information.

S&T Privacy Training and Outreach

- Conducted outreach with the new S&T Technology Foraging program (a complex process of using scientific periodicals, the Internet, and other sources to seek out technologies that are already in use or being developed, and adopting these technologies for new purposes, new environmental conditions, or at new scales) to ensure that privacy is considered for all new S&T research efforts.
- Participated in a panel discussion at the Federal Bureau of Investigation's (FBI) Facial Recognition Legal Series, discussing biometric privacy policies.
- Presented on privacy and mobile applications at two separate Lunch and Learn events hosted by NPPD and the DHS Office of Policy.
- Provided annual privacy awareness training electronically to all S&T Directorate employees and contractors. S&T Privacy trained over 2,000 S&T employees and contractors at all S&T locations during the reporting period.

Transportation Security Administration (TSA)

TSA is responsible for protecting the nation's transportation systems to ensure freedom of movement for people and commerce. TSA is most visible through its airport security screening efforts at more than 460 airports, but is also responsible for the security of other modes of transportation including highways, maritime ports, rail, mass transit, and pipelines.

During the reporting period, the TSA Privacy Office (TSA Privacy) engaged in the following activities to promote and protect privacy while supporting the work of the agency:

TSA Privacy Policy Leadership and Development

- Reviewed 387 pending contract actions to implement PII handling and breach remediation requirements where necessary.
- Provided advice on an information sharing protocol for Alien Flight Student Training with ICE to ensure appropriate collaboration in investigations while ensuring Privacy Act protections.
- Provided advice and review of the TSA Assessor Pilot to expand the use of Behavior Detection Officers (BDOs) at airport security checkpoints.

TSA Privacy Compliance

- Achieved a FISMA score of 89 percent for PIAs and 100 percent for SORNs during this reporting period.
- Completed or updated 56 PTAs, 9 PIAs and zero SORNs during the reporting period.
- PIAs and PIA updates completed included:
  - **Screening Passengers by Observation Techniques (SPOT) Program Update.** SPOT is a behavior observation and analysis program designed to provide TSA BDOs with a means of identifying persons who pose or may pose potential transportation security risks by focusing on behaviors indicative of high levels of stress, fear, or deception. The PIA update reflects the use of BDOs in pilot efforts to increase interaction with passengers at checkpoints and in sterile areas of airports.

- **Secure Flight PIA Updates.** The Secure Flight program screens aviation passengers and certain non-travelers against government watch lists before they enter the sterile area of an airport or board aircraft. The PIA updates are discussed in Section III of this report.

TSA Privacy Incident Response and Mitigation

- TSA did not experience any significant privacy incidents during this reporting period.
- Initiated a DHS data loss prevention solution to monitor email and help reduce and interdict potential privacy incidents.

TSA Privacy Training and Outreach

- Performed external outreach to privacy and civil liberties groups, including the Montgomery County, Maryland Inns of Court,[51] and the Privacy Coalition.
- Provided training at the U.S. Department of Agriculture Cybersecurity Expo, to staff at TSA's Office of Intelligence & Analysis, and at the TSA Office of Human Capital.

TSA Privacy Oversight

- Incorporated privacy compliance elements in existing audit functions performed by the TSA Office of Inspections and the TSA Office of Information Assurance and Cyber Security Division.
- Coordinated the inclusion of privacy elements in the table of penalties within the newly created Office of Professional Responsibility.

[51] These are local associations of lawyers dedicated to improving professionalism and training for the bar and bench. See: http://home.innsofcourt.org/about-us.aspx

United States Citizenship and Immigration Services (USCIS)

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

During the reporting period, USCIS Privacy engaged in the following activities to promote and protect privacy while supporting the mission of USCIS:

USCIS Privacy Policy Leadership and Development

- Issued a guidance memorandum on Using Live Data/PII for Training Purposes on October 6, 2011. The Memorandum permits programs and directorates with a substantial need to use live data in specific training environments and identifies the privacy protections and security requirements for such use of live data.
- Issued a guidance memorandum on the use of Public Key Infrastructure (PKI) for dissemination of PII on October 31, 2011. The PKI Memorandum informs USCIS employees and contractors of the requirement to use PKI encryption software and to ensure that all PII collected and disseminated by USCIS personnel is protected both within and outside of the DHS firewall. PKI allows USCIS personnel to encrypt and disseminate emails and attachments containing PII in a secure manner.
- Recruited new staff, including two Privacy Compliance Specialists, four Regional Privacy Officers (to be located in Dallas, Texas; Burlington, Vermont; Orlando, Florida; and Laguna Nigel, California), and one Staff Assistant.

USCIS Privacy Compliance

- Achieved a FISMA score of 78 percent for PIAs and 88 percent for SORNs during this reporting period.
- Completed or updated 164 PTAs, 7 PIAs and 4 SORNs during the reporting period.
- Launched the USCIS Electronic Immigration System (ELIS). Individuals can establish a USCIS ELIS account and apply online to extend or change their nonimmigrant status for certain visa types rather than apply by mail. Future releases will add form types and functions to the system, gradually expanding ELIS to cover filing and adjudication for all USCIS immigration benefits.
- Created new standard operating procedures to ensure that all external forms that collect information from the public subject to the PRA have an associated PTA.
- Established new standard operating procedures to ensure that internal forms that collect information on USCIS employees and contractors also have appropriate privacy compliance documentation.

USCIS Privacy Incident Response and Mitigation

- Managed and mitigated 261 reported privacy incidents involving a potential or actual compromise of PII. USCIS Privacy took steps to provide training and remediation to reduce risk of further privacy incidents.

USCIS Privacy Training and Outreach

- Hosted a second Annual Privacy Awareness Week from April 23-27, 2012, in partnership with the USCIS Enterprise Services Directorate Verification Division's Privacy Branch. The agenda included a variety of activities and presentations from senior USCIS and DHS leadership, as well as speakers from other agencies on how to prevent identity theft.
- Participated in the first agency-wide "National Clean–up Day," during which employees reviewed and disposed of any documents that were not federal records and were no longer needed for business purposes.
- Continued to conduct regular privacy awareness training for employees and contractors.

United States Coast Guard (USCG)

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

During the reporting period, USCG Privacy Office (USCG Privacy) engaged in the following activities to promote and protect privacy while supporting the work of the USCG:

USCG Privacy Policy Leadership and Development

- Collaborated with the USCG Information Assurance Division and promulgated new policies that:
  - Reemphasized the importance of safeguarding government emails and attachments sent to non-DHS addressees;
  - Prohibited the release of USCG Employee Identification Numbers (EMPLIDS) on the Internet.
- Partnered with the USCG Human Resources Directorate and identified protection methods to prevent privacy incidents during the civilian performance appraisal closeout and awards cycle.

USCG Privacy Compliance

- Increased its FISMA score for PIAs from 88 percent to 97 percent, and the score for SORNs similarly increased from 98 percent to 100 percent.
- Completed or updated 105 PTAs, 4 PIAs, and 4 SORNs during the reporting period.
- Updated DHS/USCG-014, Military Pay and Personnel; DHS/USCG-020, Substance Abuse Prevention and Treatment Program; DHS/USCG-027, Recruiting Files; and DHS/USCG-029, Notice of Arrival and Departure Information, during the SORN biennial review.
- Published a PIA on the Coast Guard Business Intelligence (CGBI) system. CGBI utilizes standardized enterprise data and metrics, consisting of an Enterprise Data Warehouse and a front-end business intelligence application providing standardized reports and data to USCG users.

- Published a PIA for the Composite Health Care System, a fully integrated health care information system that connects USCG medical clinics to the computerized patient records of USCG members, other military personnel, and eligible family members.
- Published an updated PIA on the Biometrics at Sea System (BASS), which is used to provide mobile biometrics collection and analysis capability at sea. BASS was modified to incorporate the USCG maritime mobile biometrics system use of Universal Serial Bus (USB) cables and encrypted hard drives instead of the encrypted flash drives to facilitate the air gap transfer of biometric and biographics from laptops to the onboard computers.

USCG Privacy Incident Response and Mitigation

The USCG Homeport Web Portal was compromised by hackers, impacting user names and passwords of approximately 20,000 accounts. The USCG Privacy Officer established the Privacy Incident Response Team (CG-PIRT) which consisted of representatives of the USCG Homeport Program/Policy Offices, Office of General Law, Public Affairs, Information Assurance, and the USCG Investigative Service. CG-PIRT collaborated with numerous government agencies and initiated remediation efforts by taking the Homeport Web Portal offline, conducting an in-depth damage assessment/risk analysis, resetting the passwords, providing notification to the impacted users, and issuing a press release.

USCG Privacy developed and disseminated the following guidance in ongoing efforts to increase privacy awareness and reduce privacy incidents:

- Promulgated policy reemphasizing the importance of safeguarding government emails and attachments to non-DHS addressees;
- Identified safeguarding methods to prevent privacy incidents during the civilian performance appraisal closeout and awards cycle; and
- Disseminated policy that prohibits the release of EMPLIDS on the Internet.

USCG Privacy Training and Outreach

- Presented Privacy Awareness/Safeguarding PII training at the USCG Civil Rights Conference, which was attended by CRCL and Equal Employment Opportunity representatives throughout the agency.
- Hosted privacy awareness training at USCG Personnel Command with representatives in attendance from the human resources community and major commands.

U.S. Customs and Border Protection (CBP)

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

During the reporting period, the CBP Privacy Office (CBP Privacy) engaged in the following activities to promote and protect privacy while supporting the work of CBP:

CBP Privacy Policy Leadership and Development

- Reviewed and provided guidance for a pilot test for electronic ocean manifest filing. The electronic filing of manifest information in the CBP pilot will ultimately reduce the costs to the trade community and the United States Government, because it eliminates paper processing, reduces the time to process exports, and provides more immediate access to export manifest information.
- Reviewed and provided guidance for the establishment of a Governance Board for the AFI. The creation of this board permits CBP Privacy to maintain a permanent role in the system development and operational use of AFI, building privacy into the program and its future evolution.
- Prepared a Privacy Compliance Memorandum for issuance by the Acting Commissioner of CBP. The memorandum, issued to all Assistant Commissioners and Executive Directors, establishes policy work flows for both privacy compliance and information sharing. The work flow for privacy compliance clarifies the process for engaging Component stakeholders in the development of PIAs and SORNs. The work flow for information sharing establishes CBP Privacy's role in clearing all information sharing agreements between CBP and external authorities. Lastly, the memorandum identifies a new responsibility through the creation of privacy liaison-staff attorney pairs for CBP's principle operational offices to integrate privacy involvement in system development and operations during the formative stage.

CBP Privacy Compliance

- Achieved a FISMA score of 22 percent for PIAs and 77 percent for SORNs during this reporting period.
- Completed or updated 37 PTAs, 6 PIAs and 4 SORNs during the reporting period.
- Examples of PIAs, SORNs and updates completed include:
  - **PIA and a SORN for AFI.** AFI is a tool CBP officials use to conduct research and analysis on existing CBP data systems to identify potential law enforcement or security risks, to develop finished intelligence products, and to streamline requests for information from AFI. CBP published the AFI PIA and SORN to notify the public of the system, to describe the potential privacy risks, and to identify the safeguards CBP has employed to mitigate those risks.
  - **PIA and SORN for ATS.** The updated PIA and SORN notify the public about the changes in ATS modules and the expansion of access to data sets used by and stored in ATS. Section III of this Report contains details on the ATS program changes.
  - **PIA and SORN for Electronic System for Travel Authorization (ESTA).** ESTA is a system that collects and maintains a record of nonimmigrant aliens who want to travel to the United States under the Visa Waiver Program, and that CBP officials use to determine eligibility to travel to the United States under the Visa Waiver Program. Because CBP added new categories of records and routine uses, the ESTA PIA and SORN notify the public of the new data elements and uses, discuss the potential privacy risks, and highlight the safeguards that mitigate those risks.
  - **SORN for the Credit/Debit Card Data System (CDCDS).** This is a system that collects, uses, and maintains records related to credit and debit card transactions CBP has with individuals. As part of CBP policy to make record keeping transparent, CBP has published the CDCDS SORN to notify the public of the system and its uses, and to describe the safeguards CBP has employed to maintain privacy.
- Prepared 578 authorization memoranda in response to requests for information from CBP systems to ensure that ad hoc information sharing complied with published routine uses for systems of records. These releases directly support federal, state, local and foreign law enforcement investigations and prosecutions.

CBP Privacy Incident Response and Mitigation

- Conducted after-hours assessments on a random number of cubicles and offices at CBP facilities within the National Capital Region to ensure the proper safeguarding of PII.
- Enforced a full lock-out of non-approved USB mass-storage devices, so that any non-approved flash drives, thumb drives, hard drives, portable music players, digital cameras, or camcorders cannot be used on any CBP workstations in any capacity.
- Managed and mitigated 58 privacy incidents involving a potential or actual compromise of PII during the reporting period.

CBP Privacy Training and Outreach

- Conducted training for the senior staff and program managers of the CBP Office of Technology Innovation and Acquisition (OTIA) on how to safeguard PII. Because of OTIA's oversight role in policy, acquisitions, and technology for all of CBP, this training will help to spread the culture of privacy throughout CBP.
- Conducted privacy training for staff members of the CBP Office of International Trade in the National Capital Region.

CBP Privacy Oversight

Beginning in May 2011, the OIG conducted an audit of CBP privacy stewardship[52] to determine if CBP has established a culture of privacy and if the Component is complying with federal privacy laws and regulations. The audit results, released in April 2012, provide three recommendations to the Acting Commissioner of CBP:

- Establish an Office of Privacy with adequate resources and staffing to ensure that CBP is able to fulfill its privacy responsibilities.
- Issue a directive that holds Assistant Commissioners and Directors accountable for their employees' understanding of and compliance with their privacy responsibilities.
- Implement stronger measures to protect employee SSNs and to minimize their use.

CBP concurred with the OIG recommendations and is taking steps to address them.

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

United States Immigration and Customs Enforcement (ICE)

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

During the reporting period, the ICE Privacy Office (ICE Privacy) engaged in the following activities to promote and protect privacy while supporting the work of ICE:

ICE Privacy Policy Leadership and Development

- Established interagency procedures for the handling of Privacy Act access or amendment requests received from the FBI Criminal Justice Information Services (CJIS). ICE works with the FBI CJIS to ensure that information from ICE, legacy Immigration and Naturalization Service, or legacy U.S. Customs Service arrests maintained in FBI records is accurate and complete.
- Issued and implemented internal agency guidance on congressional disclosures pursuant to the Privacy Act.

ICE Privacy Compliance

- Increased its FISMA score for PIAs from 72 percent during the previous reporting period to 79 percent for this reporting period. The FISMA score for SORNs similarly increased from 96 percent to 98 percent for this reporting period.[53]
- Completed or updated 50 PTAs, 11 PIAs and zero SORNs during the reporting period.
- Highlights of PIAs and PIA updates completed include:
  - **Enforce Integrated Database (EID) updates.** EID captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons

[53] The ICE SORN FISMA score increased without publication of any additional SORNs, because a system was decommissioned during the reporting period.

encountered during immigration and criminal law enforcement investigations and operations conducted by ICE, CBP, and USCIS. The two PIA updates addressed the privacy risks associated with technical upgrades and added functionality to EID and highlighted the safeguards in place to mitigate those risks.

- **ICEPIC System Updates.** ICEPIC assists ICE law enforcement agents and analysts in identifying suspect identities and discovering possible non-obvious relationships among individuals and organizations that are indicative of violations of customs and immigration laws as well as possible terrorist threats and plots. A PIA update was completed to provide transparency related to the LEIS that enables law enforcement agencies outside DHS to query certain information available through ICEPIC.
- **Alien Medical Records System.** Aliens held in ICE custody receive physical exams and treatment, dental services, and pharmacy services, depending on their medical condition and length of stay. The Alien Medical Records System PIA describes the data maintained in providing these services, the purposes for which this information is collected and used, and the safeguards ICE has implemented to mitigate the privacy and security risks to the stored PII.
- **FALCON Search and Analysis System.** This system enables ICE law enforcement and homeland security personnel to search, analyze, and visualize volumes of existing information in support of ICE's mission to enforce and investigate violations of U.S. criminal and administrative laws. This PIA discusses the privacy risks associated with such a data aggregation platform and highlights the safeguards that mitigate those risks. The PIA is discussed more fully in Section III of this report.

ICE Privacy Incident Response and Mitigation

- Resolved 124 of 141 privacy incidents that occurred during this reporting period. ICE Privacy also took steps to mitigate any damages from the incidents and to reduce the risk of future incidents.

ICE Privacy Training and Outreach

- Presented on privacy and information sharing at the Human Rights Law Conference attended by approximately 250 agents and attorneys from ICE, DHS, and DOJ.
- Discussed privacy at ICE during the Office of Professional Responsibility Leadership Conference.
- Conducted 23 training sessions on privacy and security for ICE SharePoint collaboration site users.
- Conducted a PIA writing workshop for ICE Homeland Security Investigations and ICE Office of Enforcement and Removal Operations.
- Presented on the Privacy Act, Sensitive PII, and privacy incident reporting at the Homeland Security Investigations Intelligence Manager's Conference.

ICE Privacy Oversight

The Government Accountability Office (GAO) conducted an audit of data mining systems in DHS and released a report in September 2011, recommending that the DHS Chief Privacy Officer consider shutting down LEIS until the ICEPIC PIA was updated to address the sharing of information from the ICEPIC system with external law enforcement agencies. In response to this recommendation, ICE published a PIA update addressing the external information sharing in October 2011, as noted above. The ICE Privacy Office also participated in a PCR of the ICEPIC LEIS Service, which was initiated in response to the GAO report findings and recommendation.[53] This PCR also is discussed in Section IV of this report.

[54] *http://www.dhs.gov/xlibrary/assets/privacy/privacy_privcomrev_ice-analysis.pdf*

United States Secret Service (USSS or Secret Service)

The Secret Service is mandated by Congress to carry out dual protective and criminal investigative missions. It seeks to promote a culture of privacy awareness while upholding the tradition of excellence in performing this dual mission.

During the reporting period, the USSS FOIA & Privacy Act Program (USSS Privacy), in collaboration with other offices, engaged in the following activities to promote and protect privacy while supporting the work of the Secret Service:

USSS Privacy Policy Leadership and Development

- Engaged in USSS' Information Technology Review Committee quarterly meetings to identify all newly proposed or operational systems, and facilitated engagement with project managers and program managers to ensure that privacy considerations are embedded in the design of each system.
- Reviewed and provided comments on seven USSS Social Media Directives on management of public-facing websites, standards of conduct, and guidelines for unofficial personal use of social media on non-government equipment, privacy issues, risk mitigation strategies, and legal authorities regarding the use of social media.

USSS Privacy Compliance

- Increased its FISMA score for PIAs from 25 percent during the previous reporting period to 71 percent for this reporting period. The FISMA score for SORNs is 100 percent for this reporting period.
- Completed or updated 15 PTAs, 7 PIAs and 3 SORNs during the reporting period.
- Conducted a comprehensive review of USSS FISMA systems to identify systems requiring PTAs and PIAs.
- Hired a full-time FOIA/Privacy Act Specialist to assist in the administration and implementation of statutory and regulatory requirements.
- Reviewed and drafted Privacy Act statements for new and existing USSS forms that collect PII.

USSS Privacy Incident Response and Mitigation

- Issued an official message to all USSS employees on the importance of safeguarding PII and reporting privacy incidents, and reminding employees of a dedicated phone line and e-mail address for privacy and FOIA-related inquiries and/or comments.
- Issued an official message to all USSS employees to remind employees of their responsibility to safeguard PII, Sensitive PII, and Sensitive But Unclassified Information when transmitted by email outside of USSS.
- Implemented software that provides Federal Information Processing Standard 140-2 certified full-disk encryption on all laptops issued by the Information Resources Management Division for use on the USSS network.

USSS Privacy Training and Outreach

- Provided training on "Safeguarding PII and Handling Privacy Incidents" for all administrative officers employed at headquarters and field offices at the USSS's Rowley Training Center.
- Provided training on "Safeguarding PII While Teleworking" for all USSS personnel approved to telework.
- Issued privacy awareness posters and flyers to raise privacy awareness and to encourage employees to focus on the need to protect PII.
- Created a privacy compliance brochure for dissemination at trainings and presentations.
- Enhanced the USSS intranet page to disseminate information to employees about privacy compliance, guidelines, and tools. The web page provides a basic overview of federal privacy laws and includes privacy compliance guidance materials to assist program and project managers in preparing PTAs and PIAs, and in meeting other privacy compliance requirements.

The Future of Privacy at DHS

In many ways, the future of privacy at DHS is here today. The revised DHS Privacy Office strategic plan, office realignment, and this report, all bear witness that the Office is a mature organization that both embodies and seeks to advance its vision of being a global leader in promoting and protecting privacy and transparency as fundamental principles of the American way of life.

In the coming year, the Office will continue to innovate in privacy and disclosure policy, influence through effective advocacy, integrate privacy and FOIA compliance, implement privacy oversight, inspire workforce excellence, and impact Component privacy programs and operations. The Office will address the challenges of the information age, the demands of the homeland security enterprise and the complexities of DHS itself, in order to champion privacy and transparency in DHS operations, and throughout the Federal Government.

Appendices

Appendix A–Acronym List

AFI	Analytical Framework for Intelligence
ATS	Automated Targeting System
BASS	Biometrics at Sea System
BDO	Behavior Detection Officers
CBP	U.S. Customs and Border Protection
CBSA	Canada Border Services Agency
CDCDS	Credit/Debit Card Data System
CFO	Chief Financial Officer
CGBI	Coast Guard Business Intelligence System
CG-PIRT	Coast Guard Privacy Incident Response Team
CHCO	Chief Human Capital Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CJIS	FBI Criminal Justice Information Services
CMA	Computer Matching Agreement
CRCL	Office of Civil Rights and Civil Liberties
DIB	Data Integrity Board
DHS	Department of Homeland Security
DHS TRIP	DHS Traveler Redress Inquiry Program
DOJ	Department of Justice
DPIAC	Data Privacy and Integrity Advisory Committee
EID	Enforce Integrated Database
ESTA	Electronic System for Travel Authorization
ELIS	USCIS Electronic Immigration System
FACA	Federal Advisory Committee Act
FBI	Federal Bureau of Investigation
FCC	Five Country Conference
FEMA	Federal Emergency Management Agency
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FSI	Foreign Service Institute
FY	Fiscal Year
GAO	Government Accountability Office
HSIN	Homeland Security Information Network
I&A	Office of Intelligence and Analysis
IAPP	International Association of Privacy Professionals
ICE	U.S. Immigration and Customs Enforcement

Appendix A–Acronym List

ICEPIC	Immigration and Customs Enforcement Pattern Analysis and Information Collection
IdM	Identity Management
IDENT	Automated Biometric Identification
IIR	Intelligence Information Report
ISA-IPC	Information Sharing and Access Interagency Policy Committee
ISAA	Information Sharing Access Agreement
ISCC	Information Sharing Coordination Council
ISE	Information Sharing Environment
ISE-SAR	Information Sharing Environment-Suspicious Activity Reporting
ISSGB	Information Sharing and Safeguarding Governance Board
LEIS	Law Enforcement Information Sharing Service
LE-SMC	Law Enforcement Shared Mission Community
MGMT	DHS Management Directorate
NCTC	National Counterterrorism Center
NICC	National Infrastructure Coordinating Center
NIST	National Institute for Standards and Technology
NPPD	National Programs and Protection Directorate
NSTAC	National Security Telecommunications Advisory Committee
NSTC	National Science and Technology Council
NSTIC	National Strategy for Trusted Identities in Cyberspace
NPSBN	Nationwide Public Safety Broadband Network
OIG	Office of Inspector General
OLE/FAMS	TSA Office of Law Enforcement / Federal Air Marshal Service
OMB	Office of Management and Budget
OIP	DOJ Office of Information Policy
OPS	DHS Office of Operations Planning and Coordination
OTIA	CBP Office of Technology Innovation and Acquisition
PCII	Protected Critical Infrastructure Information
PCR	Privacy Compliance Review
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIHG	Privacy Incident Handling Guidance
PKI	Public Key Infrastructure
PNR	Passenger Name Records
PPAT	Privacy Policy and Advocacy Team
PPOCs	Privacy Points of Contact
PRA	Paperwork Reduction Act

Appendix A–Acronym List

PTA	Privacy Threshold Analysis
QHSR	Quadrennial Homeland Security Review
RWG	Records Working Group
ROBC	Reports Officers Basic Course
S&T	Science and Technology Directorate
SAR	Suspicious Activity Reporting
SBA	U.S. Small Business Administration
SLPO	I&A State and Local Program Office
SOC	Security Operations Center
SORN	System of Records Notice
SSA	Social Security Administration
SSN	Social Security Number
SPOT	Screening Passengers by Observation Techniques
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

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

DHS's implementation of the FIPPs is described below: [55]

- **Transparency:** DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.
- **Individual Participation:** DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
- **Purpose Specification:** DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- **Data Minimization:** DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration.
- **Use Limitation:** DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
- **Data Quality and Integrity:** DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII.
- **Security:** DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing:** DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

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

Appendix C–Compliance Activities

The Privacy Compliance Process

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

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

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

(2) the OMB IT budget submission process, which requires the DHS Privacy Office to review all major DHS IT investments and associated systems on an annual basis, prior to submission to OMB for inclusion in the President's annual budget, to ensure that proper privacy protections and privacy documentation are in place;[56]

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

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

Privacy Compliance Documents: Keys to Transparency and Accountability

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

PTAs

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

PIAs

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

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

Appendix C–Compliance Activities

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

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

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

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 DHS Privacy Office. As with the PIA, the Chief Privacy Officer reviews, signs, and publishes all SORNs for the Department.

Periodic Reviews

Once the PTA, PIA, and SORN are completed, they are reviewed periodically by the DHS Privacy Office (timing varies by document type and date approved). For systems that require only PTAs and PIAs, the process begins again three years after the document is complete or when there is an update to the program, whichever comes first. The process begins with either the update or submission of a new PTA. OMB guidance requires that SORNs be reviewed on a biennial basis.[57]

[57] 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.*

Appendix C–Compliance Activities

Computer Matching Agreements and the DHS Data Integrity Board

Under *The Computer Matching and Privacy Protection Act of 1988*, which amended the Privacy Act, federal agencies must establish a DIB to oversee and approve their use of computer matching programs.[58] The Chief Privacy Officer serves as the Chairperson of the DHS DIB and members include the Inspector General and representatives of Components that currently have active CMA in place.[59]

Before the Department can match its data with data held by another federal agency or state government, either as the recipient or as the source of the data, it must enter into a written CMA with the other party, which must be approved by the DHS DIB. CMAs are required when there is a comparison of two or more automated systems of records for the purpose of verifying the eligibility for cash or in-kind federal benefits.[60]

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.

[58] 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).

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

[60] 5 U.S.C. § 552a(o).

Appendix D–Published PIAs and SORNs

Privacy Impact Assessments Published, July 1, 2011–June 30, 2012

Component	Name of System	Date Published
DHS-wide	DHS/ALL/PIA-027(b), Watchlist Update	7/20/2011
DHS-wide	DHS/ALL/PIA-040, Electronic Patient Care Reporting System	9/2/2011
DHS-wide	DHS/ALL/PIA-013(a), PRISM System	11/10/2011
DHS-wide	DHS/ALL/PIA-028(a), Department Freedom of Information Act and Privacy Act Records Program Update	12/22/2011
DHS-wide	DHS/ALL/PIA-041, One DHS Overstay Vetting Pilot	12/29/2011
FEMA	DHS/FEMA/PIA-014(a), National Emergency Family Registry and Locator System	8/30/2011
FEMA	DHS/FEMA/PIA-018, Suspicious Activity Reporting	9/9/2011
FEMA	DHS/FEMA/PIA-019, Firehouse Database (Classified and Unclassified) Assistance	12/16/2011
FEMA	DHS/FEMA/PIA-020, Integrated Financial Management Information System Merger	12/16/2011
FEMA	DHS/FEMA/PIA-021, Advanced Call Center Network Platform	3/26/2012
FEMA	DHS/FEMA/PIA-022, Student Training/Exercise Application & Registration Records	3/30/2012
FEMA	DHS/FEMA/PIA-023, Enterprise Coordination and Approvals Processing System	5/21/2012
FEMA	DHS/FEMA/PIA-024, Accounting Package	6/13/2012
FEMA	DHS/FEMA/PIA-027, National Emergency Management Information System-Individual Assistance Web-based and Client-based Modules	6/29/2012
MGMT	DHS/MGMT/PIA-006, E-mail Secure Gateway	3/23/2012
NPPD	DHS/NPPD/PIA-006(a), Protected Critical Infrastructure Information Management System	7/13/2011
NPPD	DHS/NPPD/PIA-019, Ammonium Nitrate Security Program	7/25/2011
NPPD	DHS/NPPD/PIA-017(a), National Infrastructure Coordination Center Suspicious Activity Reporting Initiative	8/15/2011
NPPD	DHS/NPPD/US-VISIT-PIA-007(a), Biometric Interoperability between the U.S. Department of Homeland Security and the U.S. Department of Justice	9/19/2011
NPPD	DHS/NPPD/US-VISIT-PIA-007(b), Biometric Interoperability between the U.S. Department of Homeland Security and the U.S. Department of Justice	10/13/2011
NPPD	DHS/NPPD/PIA-020, Critical Infrastructure Private Sector Clearance Program	11/2/2011

Appendix D–Published PIAs and SORNs

Privacy Impact Assessments Published, July 1, 2011–June 30, 2012

Component	Name of System	Date Published
NPPD	DHS/NPPD/PIA-021, National Cyber Security Division Joint Cybersecurity Services Pilot (JCSP)	1/13/2012
NPPD	DHS/NPPD/PIA-022, Linking Encrypted Network System	2/10/2012
NPPD	DHS/NPPD/PIA-010(a), FPS Dispatch and Incident Records Management System Update	3/13/2012
OPS	DHS/OPS/PIA-002, Homeland Security Information Network (HSIN) Sensitive But Unclassified Update	4/16/2012
S&T	DHS/S&T/PIA-023, Biometrics Access Control System at the Transportation Security Lab	7/6/2011
S&T	DHS/S&T/PIA-006, Protected Repository for the Defense of Infrastructure Against Cyber Treats Update	11/8/2012
S&T	DHS/S&T/PIA-012(a), Future Attribute Screening Technology / Passive Methods for Precision Behavioral Screening	12/22/2011
TSA	DHS/TSA/PIA-016(a), Screening of Passengers by Observation Techniques Program	8/8/2011
TSA	DHS/TSA/PIA-018(b), Secure Flight Program Update	8/15/2011
TSA	DHS/TSA/PIA-036, K-9/Canine Web Site	1/13/2012
TSA	DHS/TSA/PIA-012, Transportation Worker Identification Credential	1/16/2012
TSA	DHS/TSA/PIA-018(e), Secure Flight Program Update	4/13/2012
USCIS	DHS/USCIS/PIA-027(a), Refugees, Asylum, and Parole System (RAPS) and the Asylum Pre-Screening System Update	7/6/2011
USCIS	DHS/USCIS/PIA-006, Systematic Alien Verification for Entitlements Program	8/29/2011
USCIS	DHS/USCIS/PIA-039, Transformation	8/29/2011
USCIS	DHS/USCIS/PIA-015(a), Computer Linked Application Information Management System 4	8/31/2011
USCIS	DHS/USCIS/PIA-041, Electronic Immigration System-1 Temporary Accounts and Draft Benefit Requests	5/22/2012
USCIS	DHS/USCIS/PIA-042, Electronic Immigration System-2 Account and Case Management	5/22/2012
USCIS	DHS/USCIS/PIA-043, Electronic Immigration System-3 Automated Background Functions	5/22/2012
USCG	DHS/USCG/PIA-002(c), Biometrics at Sea Update	7/14/2011
USCG	DHS/USCG/PIA-017, Coast Guard Composite Health Care System	7/25/2011

Appendix D–Published PIAs and SORNs

Privacy Impact Assessments Published, July 1, 2011–June 30, 2012

Component	Name of System	Date Published
USCG	DHS/USCG/PIA-018, Coast Guard Business Intelligence	4/18/2012
CBP	DHS/CBP/PIA-007(a), Electronic System for Travel Authorization Fee and Information Sharing Update	7/19/2011
CBP	DHS/CBP/PIA-009(a), CBP Primary and Secondary Processing (TECS) National SAR Initiative	8/8/2011
CBP	DHS/CBP/PIA-006(b), Automated Targeting System	6/1/2012
CBP	DHS/CBP/PIA-010, Analytical Framework for Intelligence	6/7/2012
ICE	DHS/ICE/PIA-029, Alien Medical Records System	8/1/2011
ICE	DHS/ICE/PIA-030, Security Management Closed-Circuit Television System	8/4/2011
ICE	DHS/ICE/PIA-031, Alien Medical Tracking System	9/26/2011
ICE	DHS/ICE/PIA-004(a), Ice Pattern Analysis and Information Collection Update	10/26/2011
ICE	DHS/ICE/PIA-015(c), Enforcement Integrated Database Update	11/7/2011
ICE	DHS/ICE/PIA-032, FALCON Search and Analysis System	2/3/2012
ICE	DHS/ICE/PIA-006(b), Data Analysis and Research for Trade Transparency System Update	4/4/2012
ICE	DHS/ICE/PIA-015(d), Enforcement Integrated Database Update	4/6/2012
USSS	DHS/USSS/PIA-004, USSS Counter Surveillance Unit Reporting Database (CSUR)	07/27/2011
USSS	DHS/USSS/PIA-007, Forensic Services Division Polygraph System	12/19/2011
USSS	DHS/USSS/PIA-008, Advanced Imaging Technology	1/9/2012
USSS	DHS/USSS/PIA-009, Field Investigative Reporting System	3/9/2012
USSS	DHS/USSS/PIA-010, Enterprise Investigation System	4/3/2012

Appendix D–Published PIAs and SORNs

System of Records Notices Published, July 1, 2011-June 30, 2012

Component	Name of System	Date Published
DHS-wide	DHS/ALL-030, Use of the Terrorist Screening Database	7/6/2011
DHS-wide	DHS/ALL-034, Emergency Care Medical Records	8/30/2011
DHS-wide	DHS/ALL-017, General Legal Records	11/23/2011
FEMA	DHS/FEMA-001, National Emergency Family Registry and Locator System	8/30/2011
FEMA	DHS/FEMA-012, Suspicious Activity Reporting	9/28/2011
NPPD	DHS/NPPD-001, National Infrastructure Coordinating Center	10/14/2011
USCIS	DHS/USCIS-004, Systematic Alien Verification for Entitlements Program	9/21/2011
USCIS	DHS/USCIS-014, Electronic Immigration System-1 Temporary Accounts and Draft Benefit Requests	11/15/2011
USCIS	DHS/USCIS-015, Electronic Immigration System-2 Account and Case Management	11/15/2011
USCIS	DHS/USCIS-016, Electronic Immigration System-3 Automated Background Functions	11/15/2011
USCG	DHS/USCG-027, Recruiting Files	8/10/2011
USCG	DHS/USCG-020, Substance Abuse Prevention and Treatment Program	8/11/2011
USCG	DHS/USCG-014, Military Pay and Personnel	10/28/2011
USCG	DHS/USCG-029, Notice of Arrival and Departure	11/9/2011
CBP	DHS/CBP-009, Electronic System for Travel Authorization	11/2/2011
CBP	DHS/CBP-003, Credit/Debit Card Data System	11/2/2011
CBP	DHS/CBP-006, Automated Targeting System	5/22/2012
CBP	DHS/CBP-017, Analytical Framework for Intelligence	6/7/2012
USSS	DHS/USSS-001, Criminal Investigation Information	8/10/2011
USSS	DHS/USSS-003, Non-Criminal Investigation Information System	10/28/2011
USSS	DHS/USSS-004, Protection Information System	10/28/2011

Appendix E–Public Speaking Engagements

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

July 2011

- Association of Government Accountants 60th Annual Professional Development Conference & Exposition.

September 2011

- Federal Trade Commission, CIO International Privacy Subcommittee Working Group, International Privacy Training Forum, Washington, DC
- Recorded video for the 2011 Biometric Consortium Conference & Technology Expo to be made part of compilation of United States Government leaders to open the event and to recognize the 10th Anniversary of 9/11
- NCTC Data Aggregation Summit, McLean VA

October 2011

- NPPD Privacy Week

November 2011

- International Conference of Data Protection & Privacy Commissioners (multiple panelists), Mexico City

December 2011

- National Defense University
- International Association of Privacy Professionals (IAPP) Conference, Practical Privacy Series

January 2012

- Foreign Service Institute, State Department, International Privacy Policy Training for Foreign Service Officers, Washington, DC
- Homeland Security and Counterterrorism Program of the Center for Strategic and International Studies Conference (multiple panels)

February 2012

- Beyond the Border Public Experts Meeting organized by the Canada-U.S. Law Institute

March 2012

- IAPP 2012 Global Privacy Summit, Washington DC

April 2012

- Department of the Treasury, CIO International Privacy Subcommittee Records and Information Management Month Conference
- Department of Veterans Affairs Privacy Speaker Series
- USCIS Privacy Awareness Week

Appendix E–Public Speaking Engagements

May 2012

- Department of Health and Human Services Cyber Technical Exchange 3rd Quarter FY12 Meeting, Bethesda, MD
- CIO Council Privacy Committee, Subcommittee on Best Practices
- General Services Administration Quarterly training on the Federal Advisory Committee Act, Washington, DC

June 2012

- Foreign Service Institute, Department of State, Washington, DC
- Privacy Compliance Workshop (multiple presenters), Washington, DC

Appendix F–Congressional Testimony and Staff Briefings

Congressional Testimony:

The Chief Privacy Officer testified before the House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence at two hearings during the reporting period:

- "Intelligence Sharing and Terrorist Travel: How DHS Addresses the Mission of Providing Security, Facilitating Commerce and Protecting Privacy for Passengers Engaged in International Travel," on October 5, 2011; and
- "DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy," on February 16, 2012.

Congressional Staff Briefings:

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

July 2011

- Committee on Homeland Security, Subcommittee on Oversight, Investigations and Management: Update on privacy and FOIA issues.

August 2011

- Senate Select Committee on Intelligence: Information Sharing between DHS and NCTC.

September 2011

- Senate Homeland Security and Governmental Affairs: DHS support for Fusion Centers and Privacy Policy Review Process, and Information Sharing between DHS and NCTC.

October 2011

- House Committee on Homeland Security and the Science, Space, and Technology Committee, Subcommittee on Investigations and Oversight: September 2011 GAO report on DHS's data mining activities.

February 2012

- Senate Homeland Security and Governmental Affairs Committee, Senate and House Appropriations staff: CFO-led FY 2013 budget briefings.
- Senate Homeland Security Permanent Subcommittee on Investigations staff: The DHS Privacy Office's review of IIRs generated by I&A through I&A's participation with the State and Major Urban Area Fusion Centers.

March 2012

- Members of Senators Durbin and Franken's staff: Cybersecurity, privacy protection, and information sharing.

May 2012

- Members of Senator Akaka's staff: Proposed revisions to the Privacy Act.

June 2012

- Committee on Homeland Security Majority staff members: Addressed questions regarding whether PIAs are slowing implementation of certain programs.

Appendix G–International Outreach

The Chief Privacy Officer and DHS Privacy Office staff made presentations to the following international visitors during the reporting period:

- German Minister of Justice and staff
- German Ministry of the Interior staff
- German Bundestag Representatives
- German State of Bavaria Ministries of Justice and Consumer Protection
- German State of North Rhine-Westphalia Parliament Member
- German Data Protection Officer for the City of Hamburg
- Dutch Ministry of the Interior staff
- Dutch National Police Officers
- Dutch Data Protection Authority
- Canadian Privacy Commissioner
- Ukrainian Executive Office delegation and press representatives
- Finnish Administrative Parliamentary Committee and Finnish Security Police
- Japanese Institute for International Socio-Economic Studies
- Hungarian Member of the European Parliament staff