Department of Homeland Security

2015 Privacy Office Annual Report to Congress

For the period July 1, 2014 – June 30, 2015

November 10, 2015

Homeland Security

Message from the Chief Privacy Officer

November 10, 2015

I am pleased to present the Department of Homeland Security (DHS) Privacy Office's *2015 Annual Report to Congress*, highlighting the achievements of the Privacy Office for the period July 2014 - June 2015.

Since its inception in 2004, the Privacy Office has implemented its statutory mandate to ensure that privacy protections are firmly embedded into the lifecycle of homeland security programs and systems. This remarkable achievement is the result of hard work and exceptional service by the Privacy Office staff, and the vision and accomplishments of each of the former Chief Privacy Officers. DHS is a stronger and more effective Department because of their hard work.

As the Privacy Office matures, it must be agile in order to adapt to new threats, evolving priorities, and a new fiscal environment. To that end, we revised our Strategic Plan this year to reflect our vision for protecting privacy and continuing our role as the premier privacy office in the Federal Government. The new Strategic Plan ensures that our office is optimized to most effectively support the DHS missions. This report describes each of our strategic goals and our accomplishments in meeting them during the reporting period.

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

Please direct any inquiries about this report to the Privacy Office at 202-343-1717 or privacy@dhs.gov. The report and other information about the Privacy Office can be found on our website: www.dhs.gov/privacy.

Sincerely,

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

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

The Honorable Ron Johnson
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

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

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

The Honorable Patrick Leahy
Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Richard Burr
Chairman, U.S. Senate Select Committee on Intelligence

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

The Honorable Michael McCaul
Chairman, U.S. House of Representatives Committee on Homeland Security

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

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

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

The Honorable Bob Goodlatte
Chairman, U.S. House of Representatives Committee on the Judiciary

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

The Honorable Devin Nunes
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable Adam Schiff
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

Executive Summary

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

The work of the Privacy Office supports all five core DHS missions articulated in the Quadrennial Homeland Security Review,[2] as well as the important cross-cutting goal to mature and strengthen homeland security by preserving privacy, oversight, and transparency in the execution of all departmental activities. In addition, through training, outreach, and participation in departmental program development, the Privacy Office advances the guiding principles and core values outlined in the DHS Strategic Plan for Fiscal Years 2014-2018.[3]

To accomplish these strategic outcomes, the Privacy Office established four goals in its Fiscal Year 2015-2018 Strategic Plan,[4] each supported by specific and measurable objectives, and explained in detail in the chapters that follow:

- **Goal 1 (*Privacy and Disclosure Policy*)**: Foster a culture of privacy and disclosure and demonstrate leadership through policy and partnerships;
- **Goal 2 (*Education and Outreach*)**: Provide outreach, education, training, and reports in order to promote privacy and transparency in homeland security;
- **Goal 3 (*Compliance and Oversight*)**: Conduct robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all DHS activities; and
- **Goal 4 (*Workforce Excellence*)**: Develop and maintain the best privacy and disclosure professionals in the Federal Government.

[1] 6 U.S.C. § 142.
[2] http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf
[3] https://edit.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF
[4] http://www.dhs.gov/publication/dhs-privacy-office-strategic-plan-2015-2018

Key Privacy Office achievements during the reporting period are listed below under the related strategic goal. More details on each of these items, and additional achievements, can be found in the body of the report.

Goal 1: Privacy and Disclosure Policy

- Drafted a DHS Management Instruction, "Privacy Policy for DHS Mobile Applications," to ensure that appropriate privacy protections are incorporated into mobile applications developed by, on behalf of, or in coordination with the Department.
- Played a significant role in the development of new contract clauses to ensure that sensitive information that is entrusted to contractors will be adequately protected while DHS undergoes a formal rulemaking process to add this new contractual language to the Homeland Security Acquisition Regulation.
- Participated in the recently concluded negotiations of the U.S. - European Union Data Protection and Privacy Agreement with the European Commission. The intent of this agreement is to achieve a binding umbrella agreement for sharing law enforcement information pursuant to baseline standards for protecting Personally Identifiable Information exchanged between the United States and the European Union for law enforcement, criminal justice, and public security purposes.

Goal 2: Education and Outreach

- Continued to lead the Federal Chief Information Officer Council Privacy Committee, the principal interagency forum for improving federal agency privacy practices. The Committee meets monthly to review and discuss privacy topics, proposed policies, and regulations. In November 2014, the Committee hosted a one-day Federal Privacy Summit where subject matter experts shared best practices for protecting privacy and ways to improve collaboration across the enterprise. A second Privacy Summit is planned for December 2015.
- Developed and delivered a variety of ongoing and one-time privacy and transparency-related training to DHS personnel and key stakeholders, including a year-long privacy awareness campaign throughout DHS Headquarters to convey best practices for safeguarding PII in customized classroom briefings.

Goal 3: Compliance and Oversight

- Approved 47 new or updated Privacy Impact Assessments, and 27 System of Records Notices, resulting in a Department-wide Federal Information Security Management Act privacy score of 87 percent for required investment technology system Privacy Impact Assessments, and 98 percent for System of Records Notices, an improvement over last year.
- Initiated a new process for reviewing and approving investment technology system compliance as an embedded part of the security authorization process following the release of new National Institute of Standards and Technology privacy controls for investment technology systems. Beginning in 2015, no new Authorities to Operate will be granted for investment technology systems without the Chief Privacy Officer's approval.
- Modernized Freedom of Information Act processes and improved the requester's experience by creating a new eFOIA mobile application, the first in the Federal Government. By

conveying the online request process to mobile devices, requesters can now submit requests and check the status of existing requests anyplace, anytime.

- Reviewed policies and practices of the Department's collection and use of Passenger Name Records, and published a Privacy Compliance Review that found DHS to be in compliance with the terms of the 2011 Agreement between the United States and the European Union on the use and transfer of Passenger Name Records to the Department by air carriers operating flights between the United States and the European Union, as well as with the Automated Targeting System Privacy Impact Assessment and System of Records Notice.

Goal 4: Workforce Excellence

- Responded to issues identified by employees in the 2014 Federal Employee Viewpoint Survey by establishing a Staff Advisory Council as a mechanism for staff to provide advice on Privacy Office management practices.
- Several Privacy Office staff received awards for extraordinary service from senior DHS officials, including the DHS Secretary and the Under Secretary for Management.

Privacy Office

2015 Annual Report to Congress

Table of Contents

Legislative Language

This report has been prepared in accordance with section 222 of the *Homeland Security Act of 2002* (Homeland Security Act), which includes the following requirement:

6 U.S.C. § 142 (Privacy Officer)

(a) Appointment and responsibilities-

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

****

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

Background

The mission of the Privacy Office is to protect the privacy of all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. This report, covering the period from July 1, 2014, through June 30, 2015, catalogues the Privacy 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 integrated into all DHS programs, policies, and procedures. The *Privacy Act of 1974* (Privacy Act), the *Freedom of Information Act* (FOIA), and the *E-Government Act of 2002* all require DHS to be transparent in its operations and use of information relating to individuals. The Privacy Office centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight, and to support implementation across the Department. To facilitate this process, the Chief Privacy Officer is also the Chief FOIA Officer for the Department.

The Fair Information Practice Principles (FIPPs), presented in Figure 1, are the cornerstone of DHS's efforts to integrate privacy and transparency into all Department operations.[5]

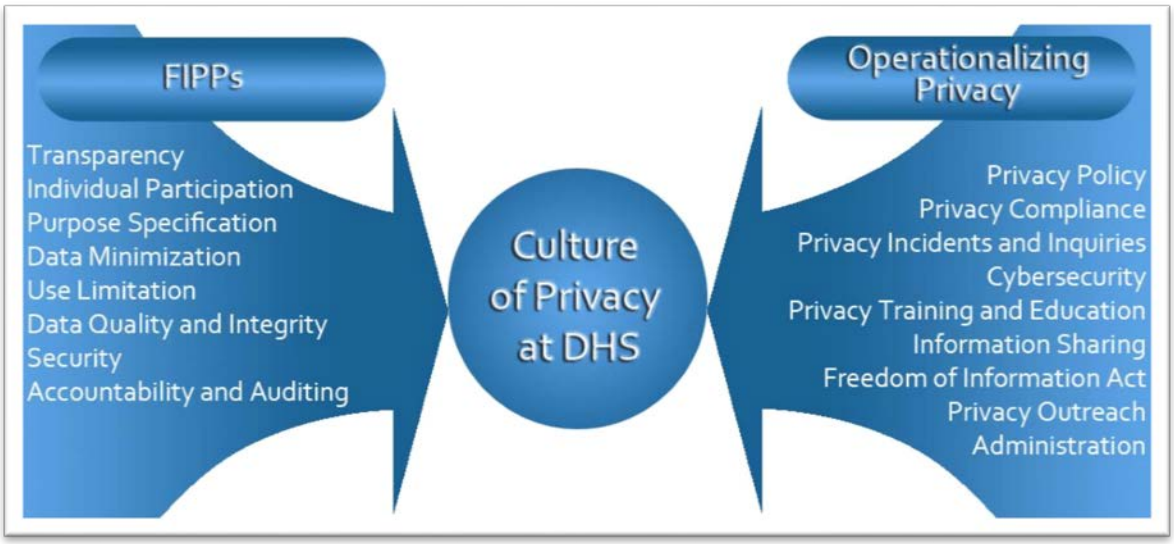


Figure 1: Privacy Office Implementation of the FIPPs

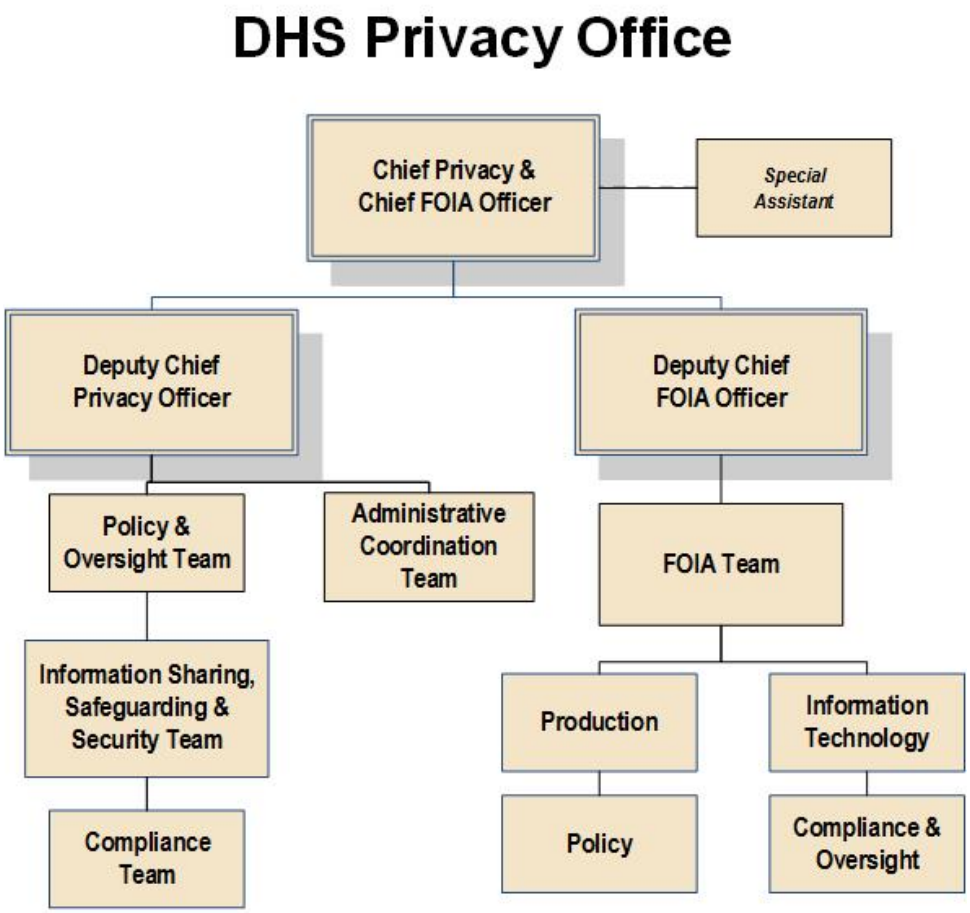
[5] The FIPPs are rooted in the *Privacy Act of 1974*, 5 U.S.C. § 552a, and memorialized in Privacy Policy Guidance Memorandum No. 2008-01, *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf,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

The Privacy Office incorporates these universally-recognized principles into privacy and disclosure policy and compliance processes throughout the Department. The Privacy Office also undertakes these statutory and policy-based responsibilities in collaboration with DHS Component privacy officers, privacy points of contact (PPOC),[6] DHS Component FOIA Officers, and program offices to ensure that all privacy and disclosure issues are afforded the appropriate level of review and expertise.

Office Structure

The recently revised organizational structure of the Privacy Office is aligned with, and accountable for, its four strategic goals as described in the Privacy Office Fiscal Year (FY) 2015-2018 Strategic Plan.[7] Figure 2 depicts the organizational structure of the Privacy Office.

Figure 2: Privacy Office Organizational Chart



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

[7] http://www.dhs.gov/publication/dhs-privacy-office-strategic-plan-2015-2018

The Privacy Office is composed of five teams:

- **Privacy Policy and Oversight Team** bears primary responsibility for developing DHS privacy policy, as well as providing subject matter expertise and support for policy development throughout the Department in areas that impact individual privacy. These areas include "Big Data," enterprise data management, cybersecurity, acquisitions and procurement, international engagement, and intelligence products. This team is also dedicated to implementing accountability and continuous improvement of DHS privacy processes and programs, in particular, the DHS Data Framework, which is DHS's Big Data solution. This team also conducts Privacy Compliance Reviews (PCR) and privacy investigations, managing the Department's privacy incident response efforts, and overseeing the Department's handling of privacy complaints. This team also supports the privacy training, public outreach, and reporting functions of the Privacy Office.

- **Privacy Compliance Team** oversees privacy compliance activities, including supporting DHS Component privacy officers, PPOCs, and DHS programs. Examples of compliance activities include the drafting of 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.

- **Information Sharing, Security and Safeguarding Team** supports the Department's information sharing activities—both domestic and international—by ensuring that privacy risks are identified, mitigation solutions are offered, and that all sharing is consistent with the DHS FIPPs. The team is well positioned to engage with operational stakeholders--as well as with oversight and policy offices--throughout the information sharing lifecycle, from evaluating new sharing requests, assessing privacy risks, crafting mitigation strategies for those risks, auditing compliance with sharing agreement's privacy protective terms and conditions, and measuring the effectiveness of those protections over time. The team also supports the Department's intelligence and homeland security enterprise through training, reviewing intelligence products, and providing policy guidance for initiatives related to, among other things, safeguarding information and preventing insider threats, countering violent extremism (CVE), and employing unmanned aircraft systems (UAS) in support of the DHS mission.

- **FOIA Team** coordinates Department-level compliance with FOIA by developing Department-wide policy needed to implement important FOIA initiatives. The FOIA Team also coordinates and oversees Component FOIA operations, provides FOIA training, and prepares required annual reports about the Department's FOIA operations. The FOIA Team also processes initial FOIA and Privacy Act requests on behalf of the Office of the Secretary (including the Military Advisor's Office and the Office of Intergovernmental Affairs (IGA)), and nine DHS Components (DHS FOIA Office Components).

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

I. Privacy and Disclosure Policy

The Office's Fiscal Year (FY) 2015-2018 Strategic Plan includes four strategic goals:

Goal One (Privacy and Disclosure Policy): Foster a culture of privacy and disclosure and demonstrate leadership through policy and partnerships.

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

Policy Initiatives

DHS Management Instruction for DHS Mobile Applications

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

Although mobile apps offer numerous benefits, there are potential privacy concerns unique to mobile app technology. These concerns include the collection, storage, use, and sharing of Personally Identifiable Information (PII), Sensitive PII, and other sensitive information such as location information, mobile device identifiers, and metadata. Additionally, mobile devices and mobile apps are vulnerable to Internet security threats, which could potentially compromise a user's information.

As a result of these concerns, the Privacy Office drafted a DHS Management Instruction, "Privacy Policy for DHS Mobile Applications," to ensure that appropriate privacy protections are incorporated into mobile apps developed by, on behalf of, or in coordination with the Department. Although the DHS FIPPs and other privacy policies provide a framework to ensure privacy protection in all Department activities, this draft Management Instruction addresses the unique privacy impacts of mobile apps to help ensure that existing policies are applied consistently to the development and use of DHS mobile apps. The Management Instruction is currently undergoing the formal Instruction review process and, once cleared, will implement DHS Directive 047-01 "Privacy Policy and Compliance" for DHS mobile apps intended for use by the public and/or by DHS employees.

Privacy Policy Leadership

During the reporting period, the Privacy Office provided significant privacy policy leadership on a wide range of topics in various fora, as described below in alphabetical order.

Automated Indicator Sharing Initiative

The Privacy Office is an active participant in the Automated Indicator Sharing (AIS) Initiative Privacy and Compliance Working Group. The Working Group includes representatives from the National Protection and Programs Directorate (NPPD) Office of Privacy, the DHS Office for Civil Rights and Civil Liberties (CRCL), as well as privacy and compliance staff from other agencies.

The AIS Initiative is an effort to develop an automated, near-real-time capability and process for the Department's National Cybersecurity and Communications Integration Center (NCCIC) to send and receive cyber threat indicators from government and non-governmental entities while ensuring the appropriate incorporation of privacy, civil liberties and other compliance protections. Partners will include federal departments and agencies, the private sector (such as private companies, academia, nonprofit organizations, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs) and other non-governmental entities), state, local, tribal and territorial partners, and foreign governmental and foreign private sector entities.

.

NPPD has primary responsibility for implementing the AIS Initiative. Nonetheless, the Privacy Office partnered with the NPPD Office of Privacy to develop privacy protections for AIS; these protections are critical to ensuring program success, and building trust with the public and DHS private sector partners. The Privacy Office will continue to participate in the AIS Privacy and Compliance Working Group as the AIS Initiative matures and develops, to ensure that the program continues to protect privacy while promoting transparency.

Biometrics Strategic Framework

As DHS transforms its management of biometrics from a Component-centric to an enterprise-wide approach, the Privacy Office is helping to promote policies and decisions consistent with the 2011 Privacy Policy Guidance Memorandum on IT Shared Services.[8] The identification of stakeholder roles such as Data Steward, Service Provider, and Data User are informing DHS's development of an enterprise vision for biometrics. These roles and the underlying policy considerations for their identification inform not only the manner in which biometrics are and will be acquired and maintained, but also the manner in which biometrics will be used and shared with DHS partners.

The recently completed DHS Biometrics Strategic Framework[9] (2015-2025) reflects these concerns in two specific ways: (1) establishing an objective to elevate biometric privacy compliance from the Component to the enterprise level, emphasizing "categorizing information according to the purpose for the original collection and sharing for compatible purposes;" and (2) promulgating another objective directing the creation of an internal DHS governance structure to prioritize and manage biometric portfolio objectives across the Department, and to preserve the "role of oversight organizations such as DHS Privacy, CRCL, and the Office of General Counsel (OGC) to ensure the execution of the strategy while continuing to protect the rights and privacy of citizens and operate within relevant legal authorities." As this governance structure is established, the Privacy Office will continue to remain an active stakeholder and participant.

[8] http://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2011-02-roles-and-responsibilities-shared-it-services

[9] https://www.fbo.gov/index?s=opportunity&mode=form&id=eecc94e7f5bb13520a0ae392b86e9c94&tab=core&_cview=0

Cyber Hygiene Working Group

The Privacy Office is an active participant in the DHS Cyber Hygiene Working Group (CHWG), which includes representatives from across DHS and its Components. In March 2015, the CHWG developed two special interim clauses, Safeguarding of Sensitive Information, and Information Technology Security and Privacy Training, which apply to new and existing contracts and solicitations that have a high risk of unauthorized access to or disclosure of sensitive information, including PII. The Privacy Office played a significant role in the development of both clauses, ensuring that they included appropriate contractor requirements for the handling of PII and Sensitive PII, incident reporting, breach notification, credit monitoring, and privacy training.

These interim clauses will ensure that sensitive information entrusted to contractors will be adequately protected while DHS undergoes a formal rulemaking process to add this new contractual language to the Homeland Security Acquisition Regulation. The Privacy Office, through the CHWG, will continue to provide support throughout the rulemaking process to ensure DHS's sensitive information, including PII, is appropriately safeguarded throughout a contract's lifecycle.

Data Framework

Through the DHS Data Access Request Council (DARC) and other working groups, the Privacy Office continues to support the development of the DHS Data Framework, a scalable information technology (IT) program that supports advanced data capabilities under formal governance processes. The Data Framework currently consists of the Neptune and Cerberus Systems and the Common Entity Index. The Data Framework uses data tags to apply policy-based rules to determine which users can access which data for what purpose, so DHS can share its information internally while ensuring that robust policy and technical controls are in place to protect privacy. This year, the Data Framework entered its Initial Operational Capability (IOC), which included the addition of more data sets and operational use of the data by a controlled set of users, and the Components were asked to accelerate movement of data sets into the framework. The Privacy Office has played, and will continue to play a significant role as data sets are prioritized, tagged, and moved into the framework.

Additionally, DHS developed an interim process to address a discrete emergent counterterrorism threat. This interim process occurs under the auspices of the Data Framework, and will revert to the standard Data Framework model when the Data Framework is capable of meeting the operational and technical requirements.

Deputy Secretary's Management Action Group

The Chief Privacy Officer participated in the Deputy Secretary's Management Action Group (DMAG), a senior leadership body that allows for candid discussion and transparent, collaborative, and coordinated decision making on a wide range of matters pertaining to DHS enterprise management, including emerging issues, joint requirements, program and budget review, acquisition, and operational planning, amongst other matters.

The Privacy Office supported the Joint Requirements Council (JRC), which reports to the DMAG, and is responsible for examining what tools and resources the Department needs in order to operate in the future across a wide variety of mission areas: aviation fleet, information-based screening and vetting equipment, information sharing systems, chemical, biological, radiological, and nuclear detection, and cybersecurity. The Privacy Office provided significant support to two portfolio groups under the JRC: Information-Based Screening and Vetting and Information Sharing Portfolio Team. These portfolio teams are responsible for evaluating various policy, resource, capability, or process issues, and providing recommendations to the JRC.

Identity, Credentialing and Access Management (ICAM) Executive Steering Committee

The Chief Privacy Officer serves as a member of the Department's Identity, Credentialing and Access Management (ICAM) Executive Steering Committee. The Privacy Office communicated closely with the Office of the Chief Information Officer's (OCIO) strategists and developers as they continued to develop the Department's consolidation and advances in ICAM services. Through ICAM's planning and technologies, OCIO plans to create a trusted identity system of integrated capabilities and supporting infrastructure to enable individuals and computer systems to verify identities through an automated trusted authentication authority at the enterprise level.

Information Sharing

The Privacy Office collaborated with Component privacy offices, the DHS Office of Intelligence and Analysis (I&A),[10] CRCL, the Office of Policy (PLCY), DHS Component data stewards, and external information sharing partners to ensure that the Department executes its information sharing programs in a privacy-protective manner.

Through these collaborative relationships, the Privacy Office:

- Provided leadership and privacy subject-matter expertise in DHS's ongoing evaluation of its information sharing with the Intelligence Community (IC).
    - As part of DHS's DARC, the Office incorporated privacy best practices, such as protections related to transparency, oversight, and redress, into Information Sharing and Access Agreements (ISAA) with the IC.
    - The Privacy Office continued to participate in quarterly reviews of the National Counterterrorism Center's (NCTC) use of DHS data, including its application of baseline safeguards.[11]
- Maintained an active leadership role in DHS's internal information sharing and management governance processes.

[10] 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.
[11] More information on NCTC's data stewardship is available through its Transparency Initiative at http://www.nctc.gov/transparency.html.

- The Privacy Office remained an active participant in the DHS Information Sharing and Safeguarding Governance Board (ISSGB) and the DHS Information Sharing Coordinating Council (ISCC).

- Through the ISCC and ISSGB, the Privacy Office supported the development of the DHS Information Sharing and Safeguarding Strategy and the DHS Information Sharing and Safeguarding Strategy Implementation Plan. The Implementation Plan includes "Priority Objective 13: Privacy, Civil Rights, and Civil Liberties Compliance Processes," which promotes enhanced privacy oversight of DHS's ISAAs and is co-led by the Privacy Office and CRCL.

- As part of the ISCC, the Privacy Office also participated in the Data Access Request Process Working Group, which seeks to memorialize and automate DHS's internal clearance processes for ISAAs and ensure that OGC, CRCL, and the Privacy Office are able to review DHS ISAAs with external entities.

- As part of the ISSGB Law Enforcement Shared Mission Community (LESMC), a Privacy Office speaker addressed over two hundred law enforcement officers from around the country at the Law Enforcement Information Sharing Initiative Annual Roundtable. By attending monthly LESMC meetings, the Privacy Office gains insight into the information sharing needs of DHS law enforcement operators and is able to engage in collaborative dialog on ways to address those needs in a privacy-consistent manner.

- As a member of the Executive Steering Committee for the DHS Office of Biometric Identity Management (OBIM), formerly known as United States Visitor and Immigrant Status Indicator Technology (US-VISIT)[12] Executive Steering Committee, the Privacy Office continued to work with OBIM to develop new processes for coordination with data owners to improve privacy and information sharing policy compliance.

- Reviewed DHS ISAAs for FIPPs-based privacy protections.

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

- Conducted quarterly reviews of United States Customs and Border Protection's (CBP) and the Transportation Security Administration's (TSA) real-time, threat-based intelligence scenarios run by the Automated Targeting System (ATS) to ensure that privacy, civil rights, and civil liberties protections were in place. ATS is an Intranet-based enforcement and

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

decision support tool used by CBP to improve the collection, use, analysis, and dissemination of information collected to target, identify, and prevent terrorists from entering the United States. The Privacy Office reviewed the intelligence scenarios four times during the reporting period.

Information sharing policy initiatives also include Privacy Office participation in two inter-agency committees:

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

  Through participation in the ISA-IPC, the Privacy Office maintains its leadership role in advancing privacy protections through the development of sound information sharing policies, both within DHS and across the Federal Government. The Privacy Office also supports ISA-IPC efforts to implement the 2013 National Strategy for Information Sharing and Safeguarding,[13] which outlines a path towards increased consistency in the application of mission-appropriate privacy, civil rights, and civil liberties protections across the ISE by building safeguards into the development and implementation of information sharing programs and activities.

- **Privacy and Civil Liberties Subcommittee:** The Chief Privacy Officer is a designated co-chair and member of the ISA-IPC Privacy and Civil Liberties (P/CL) Subcommittee, an inter-agency governance body focused on the enhancement of privacy, civil rights, and civil liberties protections in information sharing activities to support national and homeland security. The P/CL Subcommittee facilitates the adoption and implementation of policies consistent with the Information Sharing Environment (ISE) Privacy Guidelines[14] by organizations participating in the ISE.

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

[13] http://www.dhs.gov/sites/default/files/publications/12-4466-dhs-information-sharing-and-safeguarding-strategy-01-30-13--fina%20%20%20.pdf
[14] http://ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf

Information Sharing Through Biometric Interoperability

The Privacy Office partnered with the Screening Coordination Office to renegotiate biometrics-based information sharing agreements with the Department of Defense and the Department of Justice. The Privacy Office provided advice on requirements for sharing consistent with Systems of Record Notices and DHS privacy policies. These agreements are expected to be completed during the next reporting period.

International Information Sharing

The Privacy Office continues to provide subject matter expertise to the Department in its negotiation and implementation of international information sharing agreements, including projects under the US-Canada Beyond the Border Action Plan, the Five Country Conference, and Preventing and Combatting Serious Crimes Agreements.

The following are examples of projects conducted during the reporting period.

- *Data Protection and Privacy Agreement.* The Chief Privacy Officer was a member of the U.S. delegation in the recently concluded negotiations of the U.S.-European Union (EU) Data Protection and Privacy Agreement (DPPA or "Umbrella" Agreement) with the European Commission. She participated in negotiating sessions in Brussels, Belgium in July 2014 and March 2015, and in Rome, Italy in September 2014. The DPPA seeks to achieve a binding umbrella agreement for sharing law enforcement information pursuant to baseline standards for protecting PII exchanged between the United States and the EU for law enforcement, criminal justice, and public security purposes. The Chief Privacy Officer provided subject matter expertise during the negotiations to draft legislation that meets the EU's requirement that its citizens enjoy a right of judicial redress for wrongful disclosure or refusal to correct inaccurate personal information as U.S. persons – U.S. citizens and Lawful Permanent Residents – enjoy under the Privacy Act.

- *International Information Sharing Enterprise Architecture Integrated Project Team.* During the reporting period, the CIO and PLCY stood up an International Information Sharing Enterprise Architecture Integrated Project Team to advance the DHS Unity of Effort in international information sharing. As a member of this team, the Privacy Office provided input and advice on rules capabilities for a possible shared IT service solution to international information sharing.

- *DHS International Governance Board.* The Deputy Chief Privacy Officer served on the DHS International Governance Board (IGB), chaired by the Assistant Secretary for International Affairs. The IGB created a Working Group on How to Strengthen the International Affairs Enterprise in Support of DHS Missions. Privacy Office staff provided input on an evaluation of the current international affairs coordination function, and made contributions to a draft strategic plan to encourage effective coordination of new international information sharing initiatives that are consistent with privacy law and policy.

Insider Threat Program

Privacy Office Staff participate in the key working groups led by the I&A on terrorism-related issues, and have been particularly active in helping DHS develop its Insider Threat Program (ITP) this reporting year. President Obama's Executive Order 13587 requires federal agencies that operate or access classified computer networks to implement an insider threat detection and prevention program. The ITP is intended to prevent unauthorized disclosure of classified national security information, deter cleared employees from becoming insider threats, detect employees who pose a risk to classified national security information, and mitigate risks to the security of classified national security information through administrative, investigative, or other responses, while protecting the privacy, civil rights, and civil liberties of DHS personnel.

Privacy Office staff partnered with CRCL, OGC, and Office of the Chief Security Officer (OCSO) employees to create the DHS Insider Threat Oversight Group, which is responsible for providing routine oversight, advice, consultation, and assistance to the Under Secretary for Intelligence and Analysis, the Senior Insider Threat Official, the ITP Manager, and the Insider Threat Operations Center. The responsibilities of this group are defined within DHS Instruction # 262-05-002, and include reviewing any new or amended ITP strategies, policies, procedures, guidance, standards, or activities prior to their implementation. The group also conducts quarterly audits of the program to ensure that all ITP activities are conducted in accordance with applicable law and policy.

Unmanned Aircraft Systems: DHS Privacy, Civil Rights, and Civil Liberties Working Group on UAS[15]

The Privacy Office co-chairs the DHS Working Group on UAS, which was created to provide a forum for all DHS Components whose work relates in some way to UAS activities to discuss items of common interest, and to coordinate guidance on privacy, civil rights, and civil liberties issues. The Working Group has drafted a best practices document, currently in interagency clearance, that

[15] Memorandum For The Secretary from Tamara J. Kessler, Acting Officer for Civil Rights and Civil Liberties and Jonathan R. Cantor, Acting Chief Privacy Officer, "Working Group to Safeguard Privacy, Civil Rights, and Civil Liberties in the Department's Use and Support of Unmanned Aerial Systems (UAS)" September 14, 2012, https://www.dhs.gov/sites/default/files/publications/foia/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-s1-information-memorandum-09142012.pdf.

reflects the lessons learned through the Department's operation of UAS. These best practices may be used by any Component whose future plans include funding or deploying UAS, and they may also inform state and local law enforcement agencies about issues to consider when establishing a UAS program.

Data Privacy and Integrity Advisory Committee

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

- On September 22, 2014, the DPIAC held a public meeting during which DHS briefed the Committee on implementation of the DHS Data Framework, and provided an update on cybersecurity activities. The Committee then presented its research findings on privacy best practices for notice and transparency related to DHS's use of big data, and the use of audit mechanisms in the oversight process. After the meeting, the Committee's recommendations were finalized in two reports:
  1. DPIAC Recommendations Report 2014-01, Guidance on Transparency and Notice in the Department of Homeland Security Data Framework, September 22, 2014, sets forth recommendations for DHS to consider regarding notice and transparency related to the use of the DHS Data Framework, including information sharing with other agencies. (PDF, 10 pages)
  2. DPIAC Recommendations Report 2014-02, Privacy Recommendations Regarding Auditing and Oversight of the DHS Data Framework, September 22, 2014. (PDF, 14 pages)

- On May 15, 2015, the DPIAC Cyber Subcommittee was updated on pending federal cybersecurity legislation by Dr. Andy Ozment, Assistant Secretary of the Office of Cybersecurity and Communications at NPPD. Members also received a briefing on Automated Indicator Sharing.

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

[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, 5 U.S.C. App 2. DPIAC members serve as Special Government Employees and represent a balance of interests on privacy matters from academia, the private sector (including for-profit and not-for-profit organizations), state government, and the privacy advocacy community. The DPIAC provides advice on matters assigned to it by the Chief Privacy Officer and conducts its deliberations in public meetings.

II. Outreach, Education, and Reporting

The Office's FY 2015-2018 Strategic Plan includes four strategic goals:

Goal Two (Education and Outreach): Provide outreach, education, training, and reports in order to promote privacy and transparency in homeland security.

The Privacy Office ensures that the Department's privacy protections and policies are understood by every DHS employee through education and training, and are made known to the privacy community and public at large through extensive outreach.

Outreach

Advocate Meetings

The Chief Privacy Officer and Deputy Chief Privacy Officer host periodic informational meetings with members of the privacy advocacy community to inform them of key privacy initiatives throughout the year.

- *October 2014*: Dr. Andy Ozment, Assistant Secretary of the Office of Cybersecurity and Communications at NPPD, discussed cybersecurity programs at DHS, including EINSTEIN, Enhanced Cybersecurity Services, general information sharing, and incident response.
- *November 2014*: Advocates were briefed on an initial PIA regarding the use of license plate readers (LPR) at Immigration and Customs Enforcement (ICE).
- *January 2015*: Advocates were briefed on proposed federal cybersecurity legislation.
- *June 2015*: Advocates met with representatives from OGC and NPPD, who presented an overview of the Automated Indicator Sharing Initiative.

Privacy and Civil Liberties Oversight Board

The Privacy Office also participates in public and private meetings with the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency within the Executive Branch established to:

> (1) review and analyze actions the executive branch takes to protect the nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties; and
>
> (2) ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the nation from terrorism.

Examples of Privacy Office collaboration with the PCLOB during the reporting period include:

- *Privacy and Civil Liberties Assessment Report:* The Privacy Office worked closely with the PCLOB to draft this annual report, which is required by Executive Order 13636. See page 25 for more information.
- *Automated Indicator Sharing*: NPPD hosted a briefing on AIS for the PCLOB on June 10, 2015. See page 10 for more information on AIS.

Federal CIO Council Privacy Committee (Privacy Committee)[17]

The Deputy Chief Privacy Officer continued to serve as co-chair of the Federal CIO Council Privacy Committee, the principal interagency forum for improving federal agency privacy practices. The Privacy Committee serves as the interagency coordination group for Senior Agency Officials for Privacy (SAOP) and Chief Privacy Officers in the Federal Government.

The Committee meets monthly to review and discuss privacy topics, proposed policies, and regulations. During the reporting period, the Committee invited members to present on a variety of topics, including the Privacy Overlay by the Committee on National Security Systems, the White House Open Government National Action Plan 2.0 and 3.0, insider threat, federal breach legislation, data breach contracts, National Archives and Records Administration (NARA) Controlled Unclassified Information (CUI), geospatial privacy, and third party applications.

The Committee strongly supports privacy training for its members and business partners. On November 3, 2014, the Committee hosted a one-day Privacy Summit workshop that convened staff from many federal agencies in privacy, finance, procurement, IT, human resources, public affairs, congressional affairs, and intergovernmental affairs to discuss a range of privacy and security topics. Subject matter experts shared best practices for protecting privacy and ways to improve collaboration across the enterprise. A second Privacy Summit is planned for December 2015.

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

- **Best Practices Subcommittee** – This Subcommittee completed a first draft of proposed metrics for National Institute of Standards and Technology (NIST) Special Publication 800-53, Appendix J controls, and submitted them to the Department of Transportation's Office of Inspector General (OIG) for comment. The full Committee will soon review and comment on the draft metrics. Once final, the metrics will go to the NIST for review and implementation.
- **Identity Management (IdM) Subcommittee** – This Subcommittee met on April 21, 2015, to provide a briefing on the Trust Framework Solutions Component Identity Services to help inform the Subcommittee's inputs into the General Services Administration's (GSA) planned work through the Trust Framework Evaluation Team. This Subcommittee also submitted privacy-related comments on the NIST Note to Reviewers on the Electronic Authentication Guideline, 800-63-2.

[17] The Federal CIO Council was first established by EO 13011 in 1996 and later codified by Congress in the E-Government Act of 2002. The CIO Council serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of Federal Government agency information resources. *See* the CIO Council Privacy Committee website at https://cio.gov/about/groups/privacy-cop/.

- **Development and Education Subcommittee** – This Subcommittee formed a working group of agency privacy officials in 2014 to gather comments to update Office of Management and Budget (OMB) Memoranda M-07-16 and M-06-19.
- **Innovation and Emerging Technology Subcommittee** – In May 2015, this Subcommittee hosted two guest presenters from NIST to discuss NIST Special Publication 800-163, Vetting the Security of Mobile Applications (Jan. 2015). The focus was on how to automate the privacy review of mobile applications. The Subcommittee has also been busy drafting white papers, with three currently in draft on big data, data loss prevention, and biometrics.

International Engagement and Outreach

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

During the reporting period, the Privacy Office met with 31 representatives from nine countries. These engagements included briefings on the U.S. privacy framework and DHS privacy policy, privacy compliance documentation, and privacy and information sharing. Privacy Office staff also briefed outgoing U.S. diplomats deployed to foreign posts, including the U.S. Ambassador to Sweden.

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

Education: Privacy & FOIA Training and Awareness

The Privacy Office develops and delivers a variety of ongoing and one-time privacy and transparency-related training to DHS personnel and key stakeholders. In addition, the Privacy Office strives to embed a privacy module into existing training programs that involve the use or sharing of PII. DHS Components also sponsor training and awareness activities. See Chapter V for more information.

Staff Awareness

The Privacy Office e-mailed a tip sheet entitled *What You Need to Know About E-mailing Sensitive PII* to all staff to remind them of their responsibility to protect PII when e-mailing it within and outside of the DHS network.

Mandatory Online Training

Each year, DHS personnel complete the mandatory online privacy awareness training course, *Privacy at DHS: Protecting Personal Information*. This course is required for all personnel when they join the Department, and annually thereafter.

Some DHS personnel also completed Operational Use of Social Media Training during the reporting period, as required by *DHS Directive Instruction Number 110-01-001, Privacy Policy for Operational Use of Social Media*, along with any Privacy Office-adjudicated Component Social Media Operational Use Template(s) (SMOUT).

Classroom Privacy Training

- **New Employee Training:** The Privacy Office provides privacy training as part of the Department's bi-weekly orientation session for all new DHS Headquarters employees. Many of the Component Privacy Officers also offer privacy training for new employees when they onboard. In addition, the Privacy Office provides bi-monthly privacy training as part of the two-day course, *DHS 101*, which is required for all new and existing Headquarters staff.
- **Compliance Boot Camp**: The Privacy Office trained the PPOCs in compliance best practices, including how to draft PTAs, PIAs and SORNs.
- **Nationwide Suspicious Activity Reporting Initiative:** The Privacy Office provides training on privacy principles to Suspicious Activity Reporting analysts.
- **DHS 201 International Attaché Training:** The Privacy Office participates in the Department's "DHS 201" week-long training course for new DHS attachés being deployed to U.S. embassies worldwide by providing them with an international privacy policy module to raise awareness of the potential impact of global privacy policies on their work.
- **DHS Information Security Specialist Course**: The Privacy Office provides privacy training each month to participants of this week-long training program.

- **Reports Officer Certification Course**: The Privacy Office provides privacy training to reports officers who prepare intelligence reports as part of the DHS Intelligence Enterprise certification program.
- **Privacy Training for Fusion Centers**: The Privacy Office collaborates with CRCL to provide periodic privacy training for privacy officers at state and local fusion centers.
- **Privacy Briefings for Headquarters Staff**: During the reporting period, the Privacy Office launched a year-long privacy awareness campaign throughout DHS Headquarters to convey best practices for safeguarding PII in customized classroom briefings for employees and contractors.

Classroom FOIA Training

- **FOIA Records Search Training for Components and FOIA Points of Contact**: In July 2014, the Privacy Office provided FOIA Records Search Training to FOIA Officers and the designated FOIA Points of Contact responsible for gathering records. The training included a detailed explanation of the revised electronic FOIA Records Search form, a FOIA overview, and best practices for records searches.
- **FOIA Annual Report Training and Best Practices**: In October 2014, the Privacy Office provided a half-day FY 2014 Annual Report Refresher Training Workshop to the Component FOIA staff that included reporting requirements and best practices for responding to FOIA requests.
- **FOIA Training for USSS Panel Review Board:** In October 2014, the Privacy Office provided three training sessions to the United States Secret Service (USSS) Panel Review Board that included a FOIA overview and best practices for safeguarding PII.
- **FOIA Training for BioWatch Stakeholders:** In March 2015, the Privacy Office provided a FOIA training webinar to stakeholders of the BioWatch program. The training was tailored to a unique group composed of emergency first responders, state and local government offices, and the multiple federal agencies that collaborate to implement the BioWatch program.

- **FOIA Training for CIS Ombudsman staff:** In May 2015, the Privacy Office provided a FOIA overview to Office of the Citizenship and Immigration Services Ombudsman staff.

Reporting

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

- ***Privacy Office Semi-Annual Report to Congress:*** The Privacy Office issues two semi-annual reports to Congress each year as required by Section 803 of the 9/11 Commission Act,[18] as amended. 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 Privacy Office provides statistics on privacy training and awareness activities conducted by the Department.

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

- ***Chief Freedom of Information Act Officer Report to the Attorney General of the United States***: This report discusses actions taken by the Department to apply the presumption of openness and to ensure that DHS has an effective system for responding to requests, increases proactive disclosures, fully utilizes technology, reduces backlogs, and improves response times.

- ***DHS Data Mining Report to Congress***: This report describes DHS activities already deployed or under development that fall within the *Federal Agency Data Mining Reporting Act of 2007*[19] definition of data mining.

- ***Privacy and Civil Liberties Assessment Report***: Executive Order 13636[20] (EO 13636), *Improving Critical Infrastructure Cybersecurity*, requires that senior agency officials for privacy and civil liberties assess the privacy and civil liberties impacts of the activities their

[18] Pursuant to the *Intelligence Authorization Act for Fiscal Year 2014*, Pub. L. No. 113-126 (July 7, 2014), the reporting period was changed from quarterly to semiannually. The Privacy Office semiannual reports cover the following time periods: April – September, and October – March.
[19] 42 U.S.C. § 2000ee-3.
[20] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

respective departments and agencies have undertaken to implement the EO, and to publish their assessments annually in a report compiled by the Privacy Office and CRCL.

III. Compliance and Oversight

The Privacy Office's FY 2015-2018 Strategic Plan includes four strategic goals:

Goal Three (Compliance and Oversight): Conduct robust compliance and oversight programs to ensure adherence with federal privacy and disclosure laws and policies in all DHS activities.

Privacy protections are firmly embedded into the lifecycle of DHS programs and systems. In addressing new risks or adopting new and integrated approaches to protecting individual privacy, the privacy enterprise must identify early on any potential for infringement of core privacy values and protections, and address that risk accordingly. When issues are identified and resolved early, it helps ensure that programs and services provide the maximum public benefit with the least possible privacy risk.

Privacy Compliance

The Privacy Office ensures that privacy protections are built into Department systems, initiatives, projects, and programs as they are developed and modified. The Privacy Office integrates privacy into Department operations by collaborating with program or system owners and mission stakeholders across DHS during all phases of their projects. By reviewing and approving all DHS privacy compliance documentation, including PTAs, PIAs, and SORNs, the Privacy Office Compliance Team assesses the privacy risk of Departmental programs and develops mitigation strategies. The DHS PTA, PIA, and SORN templates and guidance are recognized government-wide as best practices and used by other government agencies.

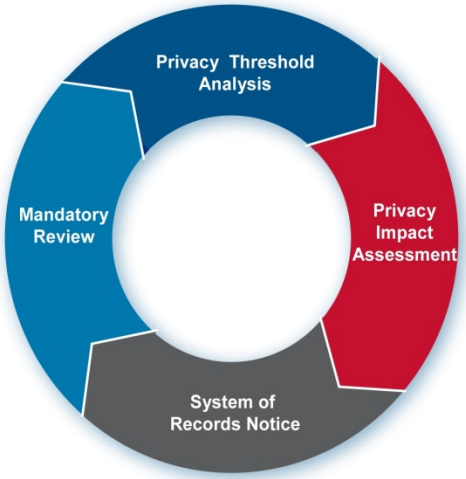


Figure 3: Privacy Office Compliance Process

The Privacy Office uses PIAs to assess risk by applying the universally recognized FIPPs to Department programs, systems, initiatives, and rulemakings. The Privacy Office also conducts privacy reviews of OMB 300 budget submissions, and supports Component privacy officers and PPOCs to ensure that privacy compliance requirements are met. The Privacy Office is responsible for ensuring that the Department meets statutory requirements such as *Federal Information Security Management Act of 2002* (FISMA)[21] privacy reporting.

The Privacy Office's 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. Illustrative initiatives during the reporting period include:

[21] 44 U.S.C. § 3541.

- The Compliance Team continued to further the Chief Privacy Officer's review of the existing PIA guidance and template. The goal is to create a document that is more streamlined and that still provides transparency and in-depth information to the public about DHS's programs, while providing a meaningful risk assessment based on the FIPPs. The Privacy Office is working with the Component privacy offices to develop new guidance that may result in a new PIA template.

- In response to strong reactions from the privacy advocacy community regarding ICE's proposed use of LPR technology, the Privacy Office was actively engaged with the DHS Front Office, United States Immigration and Customs Enforcement (ICE) Privacy Office, and ICE mission operators to build privacy safeguards into ICE's solicitation for the acquisition and use of LPR data from a commercial service in March 2015.

As of June 2015, the Department had a FISMA score of 87 percent for PIAs for required FISMA-related IT systems, and 98 percent for SORNs.

- Following the release of new NIST privacy controls for IT systems on April 1, 2014,[22] the Compliance Team initiated a new process for reviewing and approving IT system compliance as an embedded part of the security authorization process. Beginning in 2015, no new Authorities to Operate will be granted for IT systems without the Chief Privacy Officer's approval.

- The Privacy Office updated the compliance documentation and procedures for the recently issued Data Framework PIA in 2014. In 2015, the Privacy Office began adding appendices to the Data Framework PIA to provide additional transparency about the datasets being transferred and tagged for analysis. The Privacy Office will continue to update the Appendix of this PIA as more datasets are reviewed and approved through the governance process.

- The Department approved two Computer Matching Agreements (CMA). The Privacy Act requires CMAs when there is a comparison of two or more automated systems of records for the purpose of verifying the eligibility for cash or in-kind federal benefits. Additional information on CMAs is included in Appendix C.

[24] http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf

Privacy Impact Assessments

The Privacy Office publishes new and updated PIAs on its website: www.dhs.gov/privacy. During the reporting period, the Chief Privacy Officer approved 47 PIAs, and a complete list can be found in Appendix D. Figure 4 illustrates the number of approved PIAs by Component during this reporting period.[23]

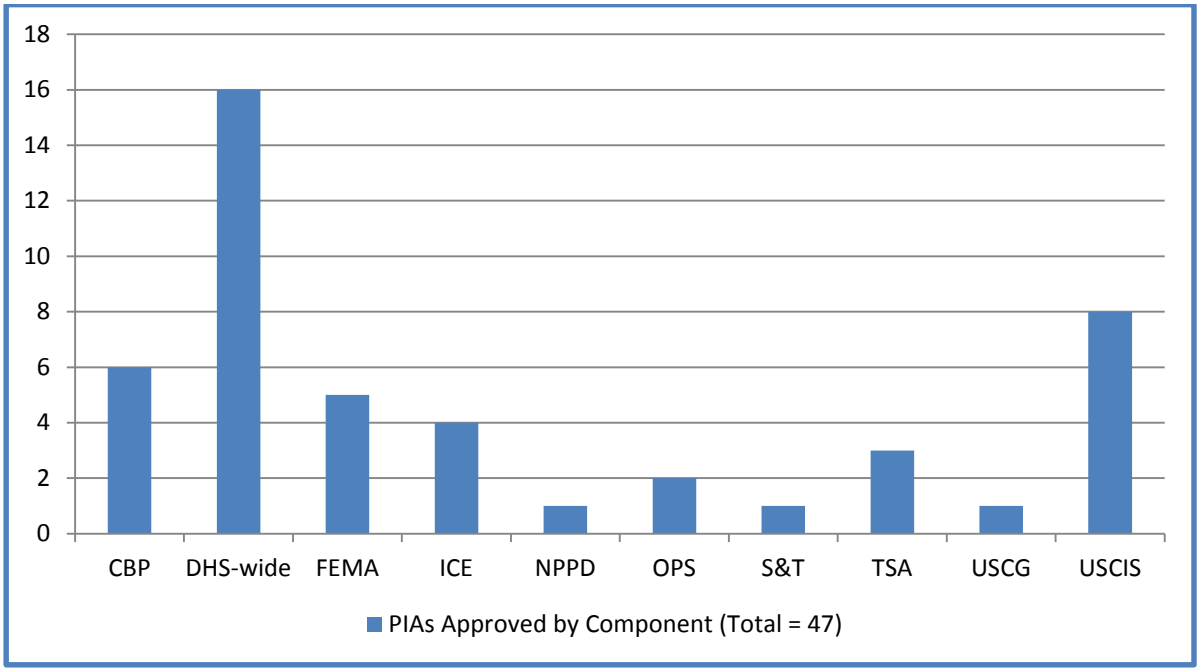


Figure 4: Number of Approved PIAs by Component during the Reporting Period

[23] This represents the total number of new or updated PIAs that were approved by the Chief Privacy Officer during the reporting period. Appendix D provides a list of approved PIAs that were published during the reporting period. A number of PIAs were approved, but not published, during the reporting period. This may occur for two different reasons: (1) the PIA was deemed to contain sensitive information (such as Law Enforcement Sensitive or otherwise classified material) and accordingly the entire document or selected portions were withheld from publication; or (2) publication of the PIA did not occur in time for the close of the reporting period. Information relating to PIAs approved but not published during the reporting period due to sensitive or classified content is being provided to Congress in a separate annex to this report.

Listed here are seven key PIAs approved during this reporting period:

1. DHS/CBP/PIA-007(d) Electronic System for Travel Authorization (ESTA) PIA

Background: ESTA is a web-based application and screening system used to determine whether certain foreign nationals are eligible to travel to the United States under the Visa Waiver Program.

Purpose: CBP published this update to the PIA for ESTA, last updated on June 5, 2013, to provide notice of changes to the ESTA application questionnaire and expansion of the ESTA application data elements. *(November 3, 2014)*

2. DHS/CBP/PIA-022 - Border Surveillance Systems (BSS)

Background: CBP's BSS are a combination of surveillance systems deployed to provide comprehensive situational awareness along the U.S. border to assist CBP in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law. BSS includes commercially available technologies such as fixed and mobile video surveillance systems, range finders, thermal imaging devices, radar, ground sensors, and radio frequency sensors.

Purpose: CBP conducted this PIA because the BSS collect and process PII including video images, photographs, radio frequency emissions, and location information. In addition, the Secure Border Initiative-net Program PIA, which addresses the Secure Border Initiative-net Southern Border and Northern Border Projects, was retired upon publication of this PIA. *(August 29, 2014)*

3. DHS/CBP/PIA-025 1:1 Face ePassport Air Entry Project

Background: CBP conducted the 1:1 Facial Recognition Air Entry Pilot to allow CBP Officers stationed at air ports of entry to use facial recognition technology as a tool to assist them in determining whether an individual presenting themselves with a valid U.S. electronic passport is the same individual photographed in that passport.

Purpose: The operational goal of this pilot is to determine the viability of facial recognition as a technology to assist Border Patrol Officers in identifying possible imposters using U.S. e-passports to enter the United States and determine if facial recognition technology can be incorporated into current CBP entry processing with acceptable impacts to processing time and the traveling public while effectively providing Border Patrol Officers with a tool to counter imposters using valid U.S. travel documents. CBP published this Privacy Impact Assessment to evaluate the privacy risks of using facial recognition software at an air port of entry.

4. DHS/CBP/PIA-026 Biometric Exit Mobile (BE-Mobile) Air Test

Background: CBP conducts a Biometric Exit Mobile Air Test for certain aliens (which generally includes all non-U.S. citizens) departing the U.S. on selected international flights at selected U.S. airports. The Biometric Exit Mobile Air Test is designed to test a new biometric exit concept of operations at selected airports. During the test, CBP officers will use a wireless handheld device at the departure gate to collect biometric and biographic data and to test outbound enforcement policies and workforce distribution procedures.

Purpose: DHS updated a previously issued PIA, entitled DHS/NPPD-001(j) Comprehensive Exit Program: Air Exit Program from 2009. The Department also transferred the privacy compliance documentation for biometric air exit programs to the CBP PIA inventory because CBP is the operational Component within the Department that is responsible for biometric and biographic entry and exit operations.

5. DHS/ALL/PIA-050 Enterprise Trusted Identity Exchange

Background: The Enterprise Trusted Identity Exchange is a privacy-enhancing DHS Enterprise Service that enables and manages the digital flow of identity, credential, and access-management data for DHS employees and contractors. It does so by establishing connections to various internal authoritative data sources, and provides a secure, digital interface to other internal DHS consuming applications. A consuming application is any DHS system that requires some form of identity, credential, and access-management data in order to grant logical or physical access to a DHS protected resource.

Purpose: DHS published this PIA because the Enterprise Trusted Identity Exchange enables and manages the digital flow of identity, credential, and access-management data for DHS employees and contractors by accessing and disseminating PII. (*April 2, 2015)*

6. DHS/ALL/PIA-051 DHS Data Framework Update: Manual Transfers for an Emergent Threat

Background: DHS has a critical mission need to perform classified queries on its unclassified data in order to identify individuals supporting the terrorist activities of: (1) the Islamic State of Iraq and the Levant (ISIL), (2) al-Qa'ida in the Arabian Peninsula, (3) al-Nusrah Front, (4) affiliated offshoots of these groups, and (5) individuals seeking to join the Syria-Iraq conflict. (These individuals are often referred to as "foreign fighters" by the media and in public discourse.) The ability to perform classified searches of unclassified data for this uniquely time-sensitive purpose will allow DHS to better identify and track foreign fighters who may seek to travel from, to, or through the United States. This type of comparison is a long-standing mission need; however, the specific threat has shortened the timeframe in which DHS must meet the need.

Purpose: DHS published this PIA to explain its plan to expedite DHS's ability to meet a critical mission need through the use of an interim manual data transfer process. (*April 15, 2015)*

7. DHS/ICE/PIA-039 Acquisition and Use of LPR Data from a Commercial Service

Background: ICE uses information obtained from LPR as one investigatory tool in support of its criminal investigations and civil immigration enforcement actions. ICE is neither seeking to build nor contribute to a national public or private LPR database.

Purpose: Because LPR information can be combined with other data to identify individuals and therefore meets the definition of personally identifiable information, ICE conducted this PIA to describe how it intends to procure the services of a commercial vendor of LPR information in order to expand the availability of this information to its law enforcement personnel. In addition, through this PIA, ICE assessed the potential impact of the use of information obtained from LPRs on the civil liberties of the public and explained the measures to be put in place to mitigate such concerns. ICE will publish an updated PIA before the commercial solution described here becomes operational. (*March 19, 2015)*

System of Records Notices

The Privacy Office publishes new and updated SORNs on its website: www.dhs.gov/privacy. During the reporting period, the Chief Privacy Officer approved 27 SORNs, and a complete list can be found in Appendix D. Figure 5 illustrates the number of SORNs approved by Component during the reporting period.

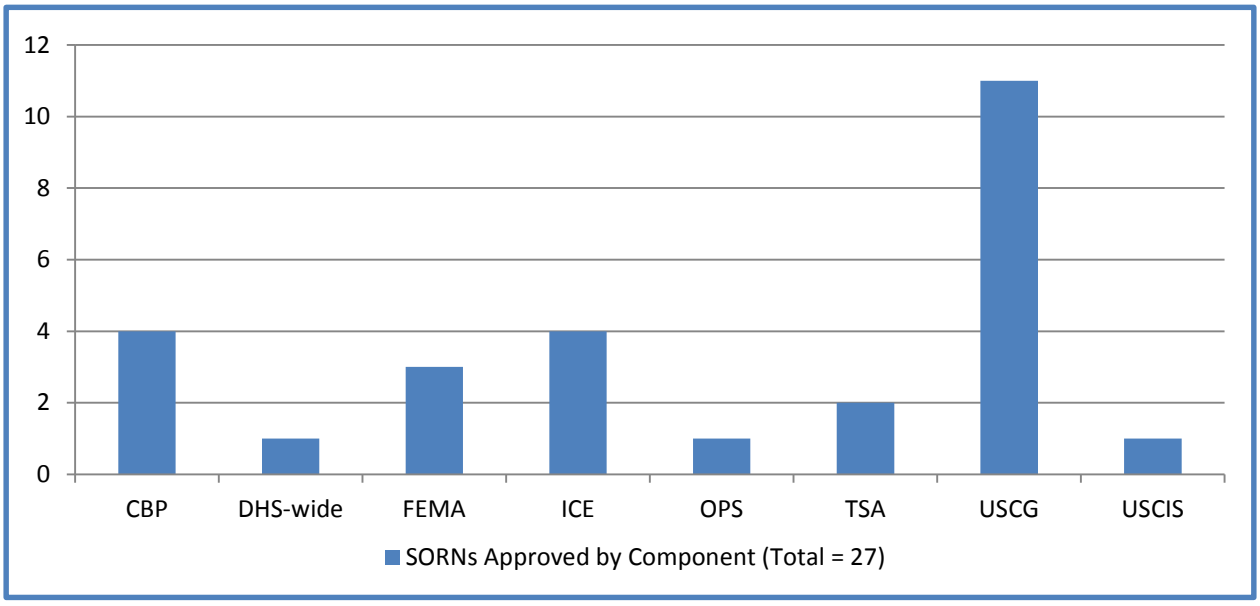


Figure 5: Number of Approved SORNs by Component during the Reporting Period

Freedom of Information Act (FOIA) Compliance

FOIA requests:[24] As in previous years, DHS continues to receive the largest number of FOIA requests of any federal department or agency in each fiscal year, receiving almost 30 percent of all requests received by the Federal Government. Since President Obama took office, DHS has experienced a 182 percent increase in the number of FOIA requests received. In fiscal year 2014, DHS received 291,242 FOIA requests, the highest number of requests to date. Most of these requests were directed to USCIS, CBP, and ICE. These Components process requests seeking immigration records, for example, copies of the Alien File, entry/exit records, and detention and deportation records.

FOIA backlog: The Privacy Office, which oversees the Department's FOIA program, partnered with CBP to eliminate the CBP backlog in 2015. The Privacy Office used its commercial off-the shelf web application solution to process requests without the need to detail employees to CBP. The Privacy Office redirected its staff to process the backlogged CBP requests, and also hired three contractors to assist in this reduction effort. As a result, the Privacy Office closed 5,014 requests at the end of FY 2014.

Due to the record-setting number of FOIA requests, the DHS backlog increased from 51,575 to 103,480 in FY 2014. Despite this increase, the Department closed 16 percent more requests in FY 2014 compared to FY 2013. In addition, 80 percent of the Components had a median processing time of less than 20 days for the 75,687 simple requests received; sixty-seven percent of the Components had average processing times of less than 20 days for simple perfected closed requests.

Components that process requests seeking immigration-related records have the largest backlogs in the Department, with CBP, ICE, NPPD, and USCIS comprising 95 percent of the total DHS backlog. The Department continued to take a multi-pronged approach to reduce its backlog, including the deployment of contractors and Privacy Office staff to the Components with the largest backlogs. Privacy Office staff also met with Component FOIA Officers and officials from other federal agencies to learn how technology, training, and staff development can help reduce the backlog, particularly through day-to-day case management. The Chief Privacy Officer and Deputy Chief FOIA Officer closely monitor the Department's caseload.

FOIA oldest requests: In FY 2014, DHS set a goal to close the Department's 10 oldest requests pending, as reported in the previous fiscal year. DHS closed eight of the 10 oldest requests in FY 2014, and 86 percent of the 10 oldest requests for each of the Components combined. DHS accomplished this through more robust oversight of departmental FOIA processing, the hard work of Component FOIA staff, consistent monitoring of FOIA-related performance measures, and a sustained effort to close the oldest requests in the backlog throughout the Department's 19 FOIA Components.

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

FOIA operations:[25] As mentioned in last year's report, the Privacy Office and several of the Component FOIA offices deployed a new electronic monitoring, tracking, and redacting commercial off-the-shelf web application solution to streamline the processing of requests and appeals under FOIA and the Privacy Act.[26] Results include: (1) increased productivity; (2) enhanced accuracy in reporting statistics, tracking cases, and better data integrity; and (3) improved interoperability and standardization of the FOIA process across the Department. During the reporting period, the Privacy Office became more proficient with the Advanced Document Review feature of the application, a de-duplication capability that allows FOIA staff to upload e-mail correspondence files and de-duplicate them.

In addition, the Components continued their efforts to foster transparency this year by proactively posting over four million pages of information to their websites.

- **Online FOIA**: DHS is working hard to improve its FOIA program by deploying advanced technology. To modernize FOIA processes and improve the customer experience, the Privacy Office partnered with the CIO and the Enterprise Systems Development Office to create the new eFOIA mobile app, which launched on July 1, 2015. By conveying the online request process to mobile devices, requesters can now submit requests and check the status of existing requests anyplace, anytime.
    - Key features of the new eFOIA app include:
        - Submit a FOIA request to any DHS Component;
        - Check the status of FOIA requests;
        - Access all of the content on the FOIA website, including the FOIA Library; and
        - Receive updates, changes to events, and recently published documents.

- DHS deployed a consolidated web-based form on its public facing FOIA website that enables requesters to submit their requests to the Department and its Components. The website explains how to submit a request and enables requesters to check the status of their requests by typing in their request numbers.

- The Privacy Office redesigned the online FOIA Library to include the libraries for NPPD, the Federal Emergency Management Agency (FEMA), and the TSA, making it easier to locate records disclosed by these Components.

FOIA Outreach - Requesters Roundtable: In March 2015, the Privacy Office hosted an open forum meeting with representatives from the Components, the Office of Government Information Services, and several members of the requester community to discuss the Department's FOIA process and ways to improve it.

[25] More detailed information on FOIA operations can be found in the *2013 Chief Freedom of Information Act Officer Report to the Attorney General of the United States*.
[26] 5 U.S.C. § 552a.

Privacy Compliance Reviews

Consistent with the Privacy Office's unique position as both an advisor and oversight body for the Department's privacy-sensitive programs and systems, the PCR was designed as a collaborative effort that helps improve a program's ability to comply with existing privacy compliance documentation, including PIAs, SORNs, and formal agreements such as Memoranda of Understanding and Memoranda of Agreement. PCRs may result in public reports or internal recommendations, depending upon the sensitivity of the program under review. Public PCR reports are available on the Privacy Office website: www.dhs.gov/privacy, under "Investigations and Compliance Reviews."

During the reporting period, the Privacy Office completed four PCRs.

Analytical Framework for Intelligence, December 19, 2014. CBP's Office of Intelligence and Investigative Liaison developed the Analytical Framework for Intelligence (AFI) to enhance DHS's ability to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk and to improve border security.

Due to the sensitive nature of the AFI system, including its search and aggregation capabilities, AFI was developed in coordination with the Privacy Office to minimize privacy risks. These privacy risks are identified and discussed in the 2012 AFI PIA. The Privacy Office also required that AFI undergo a PCR within 12 months of the system's operational deployment. The objective of this PCR was to assess compliance with the existing compliance documentation published by AFI and ensure the privacy protections in the PIA were being followed.

The Privacy Office found that the Office of Intelligence and Investigative Liaison developed AFI with privacy-protective objectives and continues to operate AFI with sensitivity to privacy and data aggregation risks. However, during the two years since AFI's launch, CBP has employed new search, analysis, and storage tools that have consolidated more data than was contemplated during the original privacy analysis in the PIA. Accordingly, the Privacy Office made 16 specific recommendations to CBP to enhance AFI privacy protections commensurate with AFI's use of these new tools.

Enhanced Cybersecurity Services (ECS) Program, April 9, 2015. ECS is a voluntary DHS program in which NPPD's Office of Cybersecurity and Communications provides indicators of malicious cyber activity to participating commercial service providers. The purpose of the program is to assist the owners and operators of critical infrastructure in enhancing their ability to protect their systems from unauthorized access, exploitation, or data exfiltration through a voluntary information sharing program. In performing the PCR, the Privacy Office found that NPPD developed the ECS Program and its related processes with privacy-protective objectives in mind. NPPD continues to operate the ECS Program and its related processes with strong

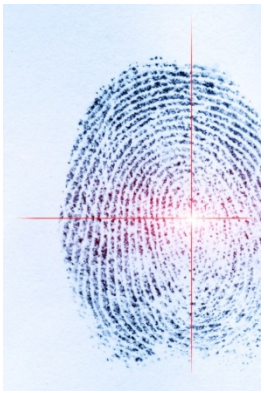
privacy oversight, which allows NPPD to identify and mitigate privacy risks as the program evolves and matures.

Media Monitoring Initiative, May 21, 2015. PCRs are a key aspect of the layered privacy protections built into the Media Monitoring Initiative to ensure that the protections described in the PIAs are followed. In February 2015, the Privacy Office conducted its seventh PCR, covering the assessment period of January 2014 – February 2015, to assess compliance with both the May 2015 PIA Update and the May 2015 SORN. The Privacy Office found that the Office of Operations Coordination, National Operations Center, continues to be in compliance with the privacy requirements identified in both of these documents and made three recommendations to continue to improve its ability to demonstrate compliance with privacy requirements.

Passenger Name Records, June 26, 2015. During the reporting period, the Privacy Office reviewed policies and practices of the Department's collection and use of Passenger Name Records (PNR) and published a final report of all findings on June 26, 2015. The review covered departmental activities from June 1, 2013 to February 1, 2015, including the details of PNR received and reviewed by DHS and information sharing practices with non-DHS entities. During the course of this PCR, the Privacy Office found PNR policies and practices, including how PNR is received, used, and disseminated by CBP, to be substantially compliant with related provisions in the Automated Targeting System PIA and SORN, making 12 recommendations to improve privacy compliance.

The review also found DHS to be in compliance with the terms of the 2011 Agreement between the United States and the European Union on the use and transfer of PNR to the Department by air carriers operating flights between the United States and the European Union (2011 Agreement). The PCR informed the discussions during joint review of the 2011 Agreement with the European Commission on July 1-2, 2015, which was hosted by the Chief Privacy Officer. During the joint review, DHS thoroughly explained DHS's use and protection of PNR, and presented its compliance with the terms of the 2011 Agreement. The European Commission will publish the results of this review by the end of 2015.

Intelligence Product Reviews



The Privacy Office reviews I&A's classified and unclassified briefings, products, reports, directives, and other materials to ensure that all reviewed work adequately protects the privacy of covered persons. During the review process, Privacy Office staff apply the FIPPs, pertinent Executive Orders, and DHS directives. Staff also participate in the key working groups led by I&A on terrorism-related issues.

During the reporting period, Privacy Office staff reviewed 762 intelligence products and 399 Intelligence Information Reports (IIR).[27]

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

Although it is not possible to review all of the IIRs produced by DHS Components, working in concert with CRCL, the Intelligence Oversight Officer, and OGC, the Privacy Office has begun auditing random samples of IIRs written by other Component's Reports Officers (RO) as resources permit. In this reporting period, Privacy Office staff audited a random sample of draft CBP and I&A RO IIRs, and found that all of them were written in a manner that adequately protected privacy.

Privacy Office staff participate in the Reports Officer Management Council (ROMC), which guides the development of ROs throughout DHS, and assists in the creation of policy related to drafting and disseminating IIRs. In addition to refining the process for certifying ROs, the ROMC tackles direct dissemination of IIRs by DHS Components, and the possible need for advanced RO training. The ROMC revised and updated the training modules for ROs in late 2014.

Privacy Incident Handling

The Privacy Office manages privacy incident response for the Department and is the author of the *DHS Privacy Incident Handling Guidance* (PIHG),[28] the foundation of DHS privacy incident response. Privacy Office staff works to ensure that all privacy incidents are properly reported, investigated, mitigated, and remediated as appropriate for each incident, in collaboration with the DHS Security Operations Center (SOC), Component privacy officers and PPOCs, and DHS management.

During the reporting period, 678 suspected or confirmed privacy incidents were reported to the DHS SOC, a decrease of 12 percent from the last reporting period. The Department investigated, mitigated, and closed 592 (87 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.

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

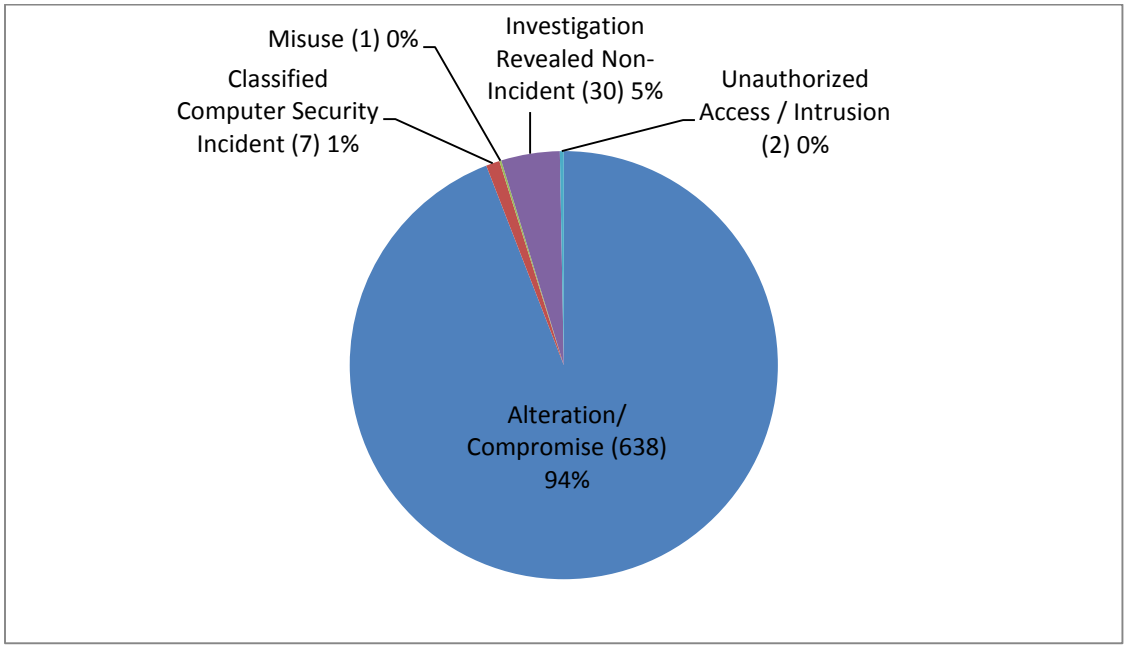


Figure 6: Percentage and Number of DHS Privacy Incidents by Type July 1, 2014 - June 30, 2015 (total = 678)[29]

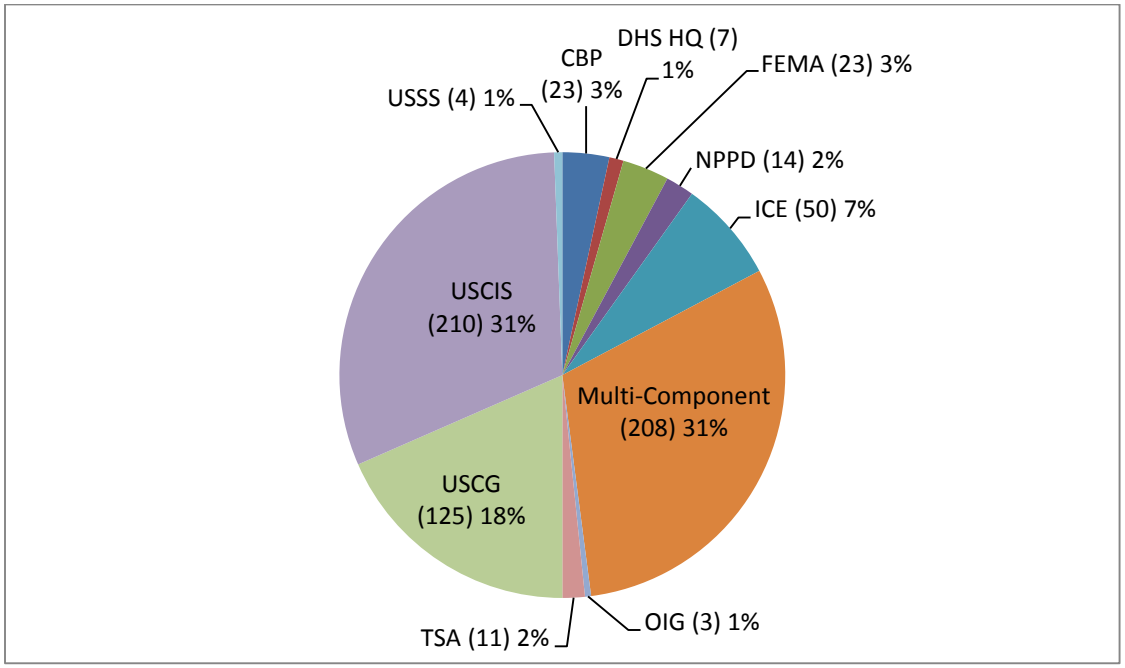


Figure 7: Percentage and Number of DHS Privacy Incidents by Component July 1, 2014 - June 30, 2015 (total = 678)[30]

[29] 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/.
[30] "Multi-Component" incidents are incidents that involve more than one DHS Component.

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

- responded to a major privacy incident affecting personnel throughout the Department by sending out notices to all impacted staff, standing up a call center to handle all inquiries, and guiding the remediation effort;
- hosted the sixth annual DHS Core Management Group Meeting in October 2014, during which stakeholders met with the Chief Privacy Officer to discuss privacy incidents and incident handling procedures;
- provided subject matter expertise to an interagency working group assisting the U.S. Office of Personnel Management in its cybersecurity incidents;
- held Privacy Incident Handling Quarterly Meetings in May and July 2015, 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; and
- provided resources on privacy incident handling to staff at the Federal Retirement Thrift Investment Board and the Department of the Navy.

Privacy Complaint Handling and Redress

The Privacy Office is responsible for ensuring that the Department has procedures in place to receive, investigate, respond to, and provide redress for complaints from individuals who contend that the Department has failed to comply with the requirements of the Privacy Act. U.S. citizens, Lawful Permanent Residents, visitors to the United States, and aliens may submit privacy complaints to the Department.[31] The Privacy Policy and 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 March 1, 2014 and March 31, 2015, the Department received 2,593 privacy complaints and closed 2,646. Figure 8 shows the categories and disposition of privacy complaints the Department received.[32]

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

[32] The semi-annual reporting period from the second and third quarters of Fiscal Year 2015was ongoing at the close of the reporting period for this Annual Report. Statistics on privacy complaints are provided in the Privacy Office's Section 803 Reports, available at http://www.dhs.gov/publication/dhs-section-803-reports-congress. For efficiency, the data reflects the reporting period used in the Section 803 Reports.

Section 803 of the *9/11 Commission Act of 2007* and OMB Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* [33] require that the Department report quarterly to Congress on privacy complaints received and their disposition. Section II of this report includes additional information on the Privacy Office's public reporting responsibilities.

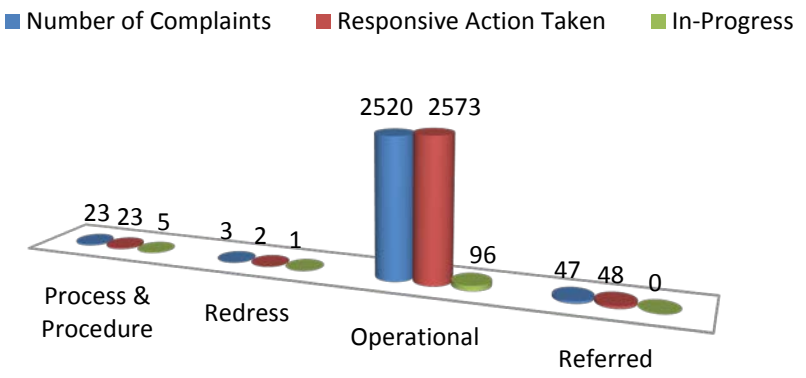


Figure 8: Privacy Complaints Received by DHS March 1, 2014 – March 31, 2015[34]

Illustrative examples of privacy complaints submitted to the Department are included in the Privacy Office's Section 803 Reports.[35]

[33] OMB Memorandum M08-21 is available at: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-21.pdf.
[34] The totals represented include complaints from previous periods that have not yet been resolved. The categories of complaints are defined in OMB M-08-21 and included in the Privacy Office's Section 803 Reports.
[35] Available at http://www.dhs.gov/files/publications/editorial_0514.shtm.

Privacy Act Amendment Requests

The Privacy Act permits an individual to request amendment of his or her own records.[36] As required by *DHS Privacy Policy Guidance Memorandum 2011-01, Privacy Act Amendment Requests*, Component privacy officers and FOIA Officers are responsible for tracking all Privacy Act Amendment requests and reporting the disposition of those requests to the Privacy Office.[37] The Policy and Oversight Team serves as the repository for those statistics. During the reporting period, the Privacy Office received zero Privacy Act Amendment requests, and three DHS Components received 78 total requests. Figure 9 shows Privacy Act Amendment Requests received by DHS during the reporting period by Component and disposition.

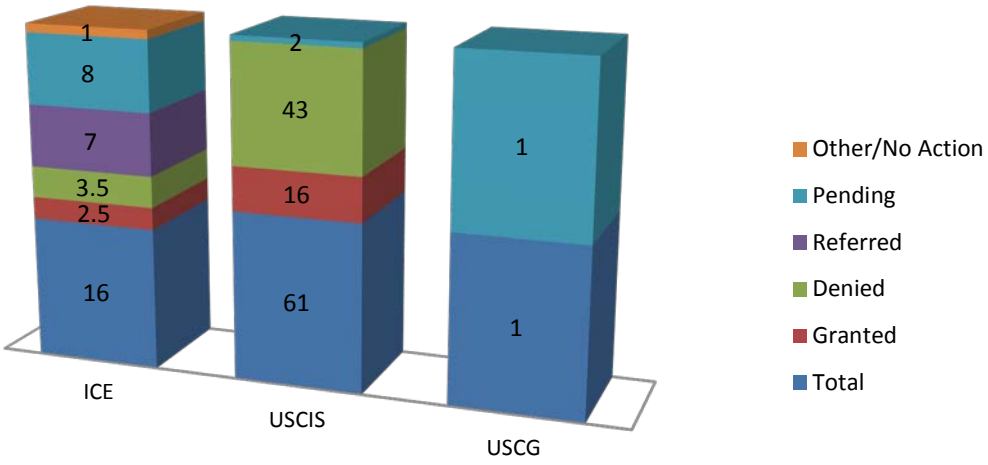


Figure 9: Privacy Act Amendment Requests by Component and Disposition July 1, 2014 - June 30, 2015[38]

[36] 5 U.S.C. § 552a(d)(2).
[37] http://www.dhs.gov/xlibrary/assets/privacy/privacy-policy-guidance-memorandum-2011-01.pdf.
[38] The total number of ICE Privacy Act Amendment Requests is less than the sum of the individual dispositions because ICE accounted for the closure of four requests that were opened in previous reporting periods.

Non-Privacy Act Redress Programs

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

- **Traveler Redress Inquiry Program (DHS TRIP)**. DHS TRIP offers one-stop redress services to the public by providing a centralized processing point for individual travellers to submit redress inquiries. Redress was developed to assist individuals who believe they have been incorrectly denied boarding, identified for additional screening, or encounter problems at customs and immigration points of entry into the country. During the reporting period July 1, 2014, through June 30, 2015, DHS TRIP received 20,181 requests for redress, with an average response time (date case opened to date case closed) of approximately 43 days.

    - The Chief Privacy Officer is a member of the DHS TRIP Advisory Board. Redress inquiries alleging non-compliance with DHS privacy policy are reviewed by the Privacy Policy and Oversight Team, and are either referred to the relevant Component, or are handled by the Privacy Office, as appropriate.

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

    - OBIM responded to 102 redress requests during the reporting period.

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

    - During the reporting period, OLE/FAMS granted 5,625 appeals and denied 208. Additionally, OLE/FAMS granted 1,367 waivers and denied 124.

IV. Workforce Excellence

The Office's FY 2015-2018 Strategic Plan includes four strategic goals:

Goal Four (Workforce Excellence): Develop and maintain the best privacy and disclosure professionals in the Federal Government.

Privacy Office staff are regarded as among the most talented privacy and disclosure professionals in the trade. This top tier talent is crucial to the Department's continued ability to implement its missions, and to its success in maintaining the public trust. These professionals have continuously demonstrated agility in responding to new priorities and fiscal environments. Providing support, opportunities for professional growth and development, and a workplace environment in which they are valued are all crucial to recruiting and retaining a high performing workforce.

Staff Training and Development

To meet this goal, the Privacy Office continuously pursues opportunities for staff professional growth and development, and fosters a workplace environment in which they are valued. Staff not only receive training from professional associations, but also are routinely asked to speak on panel discussions hosted by prominent national associations for privacy and disclosure professionals.

In addition, the Privacy Office supported staff participation in key leadership development programs this year:

- **"NextGen" Leadership Program**: One staff member completed this prestigious DHS program, which offers participants a one-year intensive leader-led development curriculum, building the next generation of talent through interaction with high-level decision makers, workshops, and team assignments. Supported by executive sponsors, participating employees explore current and emerging organizational challenges to gain a horizontal viewpoint of the Department while building key leadership skills.

- **Senior Executive Service Candidate Development Program**: Another employee was selected for this highly competitive program, which involves an intensive academic component and developmental assignment carried out in accordance with rigorous Office of Personnel Management standards.

Staff Advisory Council

In an effort to address issues identified by employees in the 2014 Federal Employee Viewpoint Survey, the Chief Privacy Officer established a Staff Advisory Council (SAC) in October 2014 as a mechanism for staff to provide advice on Privacy Office management practices. In standing up the SAC, the Chief Privacy Officer appointed seven members and tasked them with making recommendations on areas where improvement may be needed. The SAC was formalized via a charter to facilitate its function as an enduring source of support for Privacy Office staff, and a useful advisory body for future Chief Privacy Officers.

Employee Awards

One SAC recommendation was to establish an employee awards and recognition program. As a result, the Chief Privacy Officer established a program to recognize significant employee accomplishments. The program includes the Chief Privacy Officer Achievement Award and the Outstanding Service Commendation.

In addition, several Privacy Office staff received the following recognition for extraordinary service from other senior DHS officials, including from the DHS Secretary, and the Under Secretary for Management:

- **The Secretary's Award for Excellence** recognizes achievement or innovation by an individual or team engaged in work to advance the mission of the Department. The work of the nominee(s) may have resulted in superior performance, significant operational improvements or notable innovation in support of DHS missions. Three Privacy Office staff were awarded for developing the DHS Data Framework, which fosters more controlled, effective and efficient use of homeland security-related information across the Department and, as appropriate, the U.S. Government, while protecting privacy. The related systems were delivered on schedule, for multiple millions of dollars under the original estimates. Through creative use of government software, the team also delivered 35 times the proposed storage space.

- Two staff members received the **Secretary's Award for Excellence** for contributing to the Biographic Visa and Immigration Information Sharing Team. The Beyond the Border Action Plan, announced by President Obama and Canadian Prime Minister Harper in 2011, charged the U.S. government, led by the Departments of Homeland Security and State, and the Canadian government to establish a bi-directional, automated information sharing capability to assist in the effective administration and enforcement of the countries' respective immigration laws. To accomplish this objective, the team negotiated the strategic and operational efforts necessary to implement the first automated immigration information sharing initiative between the United States and Canada. As a result, consular officers and immigration officials in both countries now have the ability to make automated queries to each other to receive relevant information on certain individuals applying for admission, a visa or other immigration benefit, or who are the subjects of an investigation. As part of the Privacy Office's support for this project, the Biographic Visa and Immigration Information Sharing with Canada PIA was published in February 2014.

- The **Cross-Management Collaboration Award**, issued by the DHS Under Secretary of Management for standing up the Privacy Incident Response Center following a significant data breach. This recognition speaks not only to the exceptional work key staff have performed this past year, but also the remarkable breadth of special assignments they took on.

- The **"One DHS" Partnership Award**, issued by the DHS Under Secretary for Management for participation in the Cyber Hygiene Working Group, a joint Chief Information Officer/Chief Acquisition Officer working group that developed a government-wide cyber hygiene approach and special clauses that senior officials outside DHS used as the framework for a broad, government-wide initiative.

- A senior executive in the Privacy Office received a **"FedScoop 50" award as FedMentor of the Year**. This prestigious award was granted to only five leaders in the entire Federal Government for mentoring the next generation of leaders by providing best practices, tips, and career advice.

V. Component Privacy Programs

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

Federal Emergency Management Agency (FEMA)

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

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

Privacy Policy Leadership

- Served on FEMA's Strategic Leadership Steering Committee and Integrated Project Team for FEMA's agency-wide Workplace Transformation Initiative. With the Agency's immersion in workplace transformation, there has been increased interest in how information is being handled, shared, stored, and protected in the new FEMA open environment. As a result, the culture of privacy awareness has shifted and the Privacy Officer is consistently consulted on senior level strategic initiatives and newly proposed policy that impacts personal privacy.
- Served on the Information Governance Working Group (IGWG), representing privacy policy on the use of FEMA SharePoint sites. The IGWG helps to ensure that proper privacy

signage is in place to remind employees how to safeguard PII when posting it on SharePoint sites.
- Established a process for reporting moderate to high level privacy incidents to senior executives within the agency. This new process establishes a level of visibility into privacy incident response and mitigation, and keeps senior leadership apprised of high level incidents that could have cross-cutting impact.
- Supported the following governance boards and working groups:
    - FEMA's Acquisition Review Board, where all decisions are made regarding FEMA's procurements involving PII;
    - FEMA's Data Governance Board, where all decisions are made regarding the use of the agency's data assets involving PII;
    - FEMA's IT Governance Board, where all decisions are made regarding the use of the agency's IT assets involving PII; and
    - FEMA's Policy Working Group, to ensure that all policies are developed to minimize privacy impacts.

Privacy Compliance

- Achieved a FISMA score for SORNs of 98 percent, and maintained a FISMA score of 93 percent for PIAs during this reporting period.
- Completed or updated 165 PTAs, 5 PIAs, and 3 SORNs during the reporting period.
- Completed 187 PTAs as part of FEMA's Privacy Compliance Undocumented System Initiative, and the subsequent FEMA-wide OCIO Resiliency Project.
- Conducted a Privacy Compliance Site Assessment at the Region VI Office and the National Processing Service Center, both located in Denton, Texas.

Highlights of privacy compliance documents:

All FEMA PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

- Published a PIA on the Grant Management Program, covering 16 information collection requests and five agency IT systems.
- Published a PIA on the beta version of the Deployment Tracking System, the new IT system that maintains FEMA's deployment-related information.
- Published a PIA on the Electronic Fingerprint System to address FEMA's use of NPPD/ OBIM's Automated Biometric Identification System (IDENT) to store fingerprints as a part of its background investigations.

Privacy Training and Outreach

- Continued a FEMA National Capital Region (NCR)-wide privacy training and site risk analysis campaign in support of the agency's Workplace Transformation Initiative to co-locate FEMA personnel within the NCR, and reduce the agency's office space footprint.
- Provided Privacy Compliance Foundations training to Office of Information Technology Information System Security Officers (ISSOs), Information System Security Managers, system owners, program/project managers, and attorneys across FEMA's program offices, Regional Offices, and National Processing Service Centers. The goal is to enhance the quality of privacy compliance documents submitted by the above referenced information professionals, limit review iterations, and expedite the clearance and approval process.
- Held quarterly collaboration meetings and targeted training sessions for FEMA Privacy Points of Contacts to ensure there is a FEMA-wide focus on accurate and timely incident reporting, enforcement of mandatory annual privacy training, and identifying and reporting privacy-sensitive systems that require privacy assessment and/or documentation.
- Delivered privacy training to the disaster relief workforce at the Region VI Office, as well as the National Processing Service Center, both located in Denton, Texas.
- Enhanced the FEMA Privacy intranet Web page with a more user-friendly format, enabling employees to locate privacy-related information.
- Disseminated privacy reference materials, posters, and broadcast e-mail messages to highlight best practices for protecting PII, and reporting and mitigating privacy incidents.
- Provided privacy awareness training to all new FEMA employees in the NCR.

Federal Law Enforcement Training Centers (FLETC)

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

FLETC's FOIA & Privacy Program Office engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

Partnered with IT colleagues to ensure that privacy compliance was embedded in IT development by participating in all IT Integrated Project Teams and providing input to all System Engineering Life Cycle review boards.

Privacy Compliance

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

All FLETC PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

Privacy Training and Outreach

Provided privacy training to all FLETC IT staff.

National Protection and Programs Directorate (NPPD)

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

Privacy Policy Leadership

- Completed four Quarterly Privacy Reviews (QPR) on the handling of PII by the Cybersecurity and Communications Center (CS&C), the National Cybersecurity & Communications Integration Center (NCCIC), and the United States Computer Emergency Readiness Team's (US-CERT), resulting in: (1) the addition of Cyber Information Sharing and Collaboration Program (CISCP) indicators to the QPR review population; (2) the issuance of two high level US-CERT work instructions for EINSTEIN Monitoring and Signature Handling; and (3) the addition of a PII cover page when PII may be present in NCCIC or US-CERT products or working documents.
- Participated in Privacy Office assessments of NPPD activities under EO 13636, as well as the ECS PCR.
- Conducted two PCRs: (1) NPPD/CS&C/NCCIC's use of Twitter for the purposes of enhancing situational awareness of cyber threat activities related to government agencies, critical infrastructure and significant national events; and (2) the Information Technology Acquisition Review (ITAR) process to ensure that privacy sensitive contracts identified by the privacy subject matter experts included the required privacy provisions in the final approved and awarded contracts/Statements of Work.

- Conducted office inspections to remind employees to keep their workstations locked while they are away from their offices, and to keep their PIV cards with them at all times. Reminders were left at unattended, unlocked workstations.

In addition, NPPD's Director and Senior Privacy Officer provided leadership, serving as co-chair, to the Federal CIO Council Privacy Committee's Identity Management Subcommittee.

Privacy Compliance

- Maintained a FISMA score of 100 percent for both PIAs and SORNs during this reporting period.
- Completed or updated 32 PTAs and one PIA during the reporting period.
- Completed five Privacy Act Statements and three Paperwork Reduction Act packages.
- Conducted 148 privacy reviews as part of the ITAR process to ensure that all IT acquisitions included core privacy provisions whenever contracted services may involve access to PII.

All NPPD PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

Privacy Training and Outreach

NPPD Privacy conducted the following training and awareness events:

- Hosted quarterly privacy awareness events:
  - September 2014: Federal Trade Commission officials discussed ways to prevent and mitigate identity theft.
  - December 2014: Annual Privacy and Technology Workshop, an interactive technology demo/fair presented by various NPPD program offices to educate employees on IT security, privacy, malware, and encryption.
  - March 2015: Four-day *Privacy Training Days* event, targeting employees and contractors in the NCR.
  - May 2015: Counterintelligence (CI) Awareness Briefing to educate employees on the potential intelligence collection threat directed against DHS personnel and resources.
- All NPPD personnel completed the mandatory annual online course, *Privacy at DHS: Protecting Personal Information.*
- Developed a new Social Media Requirements Training Course that provides an overview of privacy risks associated with the use of social media, as well as DHS policy, how to gain access, roles and responsibilities, and general rules of behavior for social media use.
- Delivered Privacy Requirements for Operational Use of Social Media training to the FPS, the Office of Compliance and Security (OCS), and CS&C NCCIC.
- Provided Privacy Awareness training to Federal Protective Service FOIA personnel across all 11 regions in Kansas City, Missouri.
- Provided 11 cybersecurity information handling privacy training sessions to employees and contractors in CS&C.
- Provided Privacy 101 training for IP staff.
- Conducted privacy training for contractors supporting the replacement biometric system.

NPPD also conducted the following outreach activities:

- August 14, 2014: NPPD participated in an informal meeting with the PCLOB, hosted by CRCL, to provide an overview of the Department's cybersecurity activities and oversight. NPPD's Under Secretary and Assistant Secretary for Cybersecurity & Communications delivered remarks and discussed compliance best practices to consider in automated cybersecurity information sharing systems.
- September 22, 2014: NPPD's Assistant Secretary for Cybersecurity & Communications provided a DHS Cybersecurity Overview to the DPIAC.
- September 23, 2014 and May 15, 2015: NPPD provided various program updates to the DPIAC Cyber Subcommittee, and discussed the continuous evaluation of DHS's technical and policy approach to cybersecurity initiatives.
- March 25, 2015: NPPD Senior Privacy Officer moderated a panel entitled "The Why Behind Complex Privacy Controls" at the *Connect: ID Conference*—a conference on biometrics and identity management in Washington, D.C.
- June 9, 2015: NPPD Privacy Deputy Director participated on a panel entitled "Building Privacy Awareness" at the Department of Veterans Affairs inaugural "Privacy Matters Symposium: A Conversation in Privacy."

Office of Intelligence and Analysis (I&A)

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

I&A Privacy engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Participated in the DHS UAS Working Group to examine the privacy implications of expanded use of UAS.
- Joined other privacy colleagues and information technology experts in developing processes and procedures to establish the Department's Data Framework initiative.
- Supported I&A's efforts to implement President Obama's cybersecurity initiative embodied in EO 13636 and Presidential Policy Directive 21.
- Participated in the Watchlisting Cell Working Group to ensure that appropriate privacy protections are embedded in Department watchlisting activities.
- Supported the DARC, the coordinated oversight and compliance mechanism for the review of departmental initiatives and activities involving the internal or external transfer of PII in bulk. The goal is to ensure that such initiatives or activities comply with applicable law, and adequately protect the privacy, civil rights, and civil liberties of the individuals whose information may be shared through those initiatives or activities.

Privacy Compliance

- I&A, as an element of the Intelligence Community, is exempt from FISMA reporting requirements.
- Completed or updated 11 PTAs during the reporting period.
- Continued to ensure that all privacy requirements are met on SharePoint sites.
- Partnered with the CIO to ensure that privacy documentation is in place before any new IT investment is approved.

Privacy Training and Outreach

- Trained 1,000 personnel on Executive Order 12333, *U.S. Intelligence Activities*. The training included a discussion of privacy requirements and an overview of best practices to advance constitutional and statutory protections.
- Published notices in internal communications to remind personnel about their obligations pursuant to the Privacy Act, especially the need to remain vigilant in protecting PII.

Science and Technology Directorate (S&T)

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

In 2015, S&T, via the Cyber Security Division, initiated a privacy research program that will support DHS Privacy Office goals today and in the future.

The S&T Privacy Office (S&T Privacy) engaged in the following significant activities during this reporting period:

Privacy Compliance

- Achieved a FISMA score of 100 percent for both PIAs and SORNs during this reporting period.
- Completed or updated 25 PTAs and 1 PIA during the reporting period.

Highlights of privacy compliance documents:

All S&T PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

- Published a PIA for the Centralized Hostile Intent Project, which collects video images of trained actors posing as passengers, as well as members of the traveling public at the Theodore Francis Green Memorial State Airport in Providence, Rhode Island. The program

assesses whether behavioral indicators of malicious intent can be observed by trained professionals via video.

Privacy Training and Outreach

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

- Building Privacy Into Big Data Projects, S&T Big Data Workshop
- Disruptive Technologies & Privacy, USCIS
- Privacy & Information Security Webinar, S&T
- Privacy & The Internet of Things, USCIS
- Drones and Privacy, Information Security and Privacy Advisory Board
- Privacy and Rapid DNA Testing, S&T Workshop
- Privacy and the S&T Organizational Health Assessment Survey
- Disruptive Technologies & Privacy, National Reconnaissance Office, Privacy Awareness Week
- Privacy & Body Worn Cameras, International Association of Privacy Professionals (IAPP) webinar

Transportation Security Administration (TSA)

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

The TSA Privacy Office (TSA Privacy) engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Reviewed 295 pending contract actions to implement PII safe handling and breach remediation requirements and ensure that any other privacy compliance requirements implicated by the contract were completed.
- Provided continuous advice and oversight on passenger screening protocols, security technology initiatives, and information sharing initiatives.
- Provided advice on risk-based screening proposals and TSA Pre✓™ expansion; updated a Management Directive on requests for Secure Flight data; and drafted a Management Directive on protection for *Violence Against Women Act* section 1367 information.

Privacy Compliance

- Achieved a FISMA score of 97 percent for PIAs and 100 percent for SORNs during this reporting period.
- Completed or updated 42 PTAs, 3 PIAs and 2 SORNs during the reporting period.
- Monitored privacy compliance elements within audit functions performed by the TSA Management Control Oversight Program for internal controls at all TSA offices, to include periodic self-inspection of hard-copy and electronic data security and document destruction practices.
- Reviewed 42 programs to validate existing privacy compliance documentation.

Highlights of privacy compliance documents:

All TSA PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

- Published a PIA on the Security Threat Assessment for Conditional Access to Sensitive Security Information program. TSA occasionally discloses Sensitive Security Information (SSI) to individuals so that they can assist with the design, implementation, or review of TSA security programs, techniques, or technology, or when needed to understand TSA functions. TSA may conclude that the individuals must undergo a security threat assessment as a condition of being granted access to the SSI.
- Published a PIA Update for the Secure Flight Program. This program screens aviation passengers and certain non-travelers before they access airport sterile areas or board aircraft. TSA updated the PIA to reflect, among other things, the incorporation of risk-based assessments generated by aircraft operators using data in their existing computer-assisted passenger pre-screening systems.
- Published a PIA Update for the Alien Flight Student Program. TSA conducts Security Threat Assessments on individuals who are not U.S. citizens or nationals, as well as other individuals designated by TSA seeking flight instruction or recurrent training from Federal Aviation Administration-certified flight training providers. This update reflects that: 1) TSA performs recurrent vetting of covered individuals; 2) the defense attaché collects biographic information and creates a record in the Alien Flight Student Program about foreign military pilots endorsed by the Department of Defense for flight training in the United States; and 3) TSA has submitted an updated National Archives and Records Administration schedule to change records retention to 80 years in order to permit TSA to comply with a requirement that it re-use fingerprints for recurrent flight training during the life of the covered individual.

Privacy Training and Outreach

- Reached out to a variety of privacy and civil liberties groups and thought leaders, including the American Civil Liberties Union, Federal CIO Council Privacy Committee, American Arab Anti-Discrimination Committee, CATO Institute, and The George Washington University Cybersecurity and Aviation Roundtable.
- Trained staff on the safe handling of PII at TSA's Office of Intelligence & Analysis, Office of Human Capital, Office of Law Enforcement (Personnel Security Division), and ISSOs.
- Trained Sensitive Security Information Coordinators in privacy.
- Disseminated a monthly newsletter to TSA personnel and the Department's Privacy Points of Contact with information on privacy-related topics, including best practices to safeguard PII.
- Distributed broadcast emails to staff on how to safeguard medical and financial information.
- Assisted over 300 travelers and employees by responding to questions about TSA programs and screening requirements.

United States Citizenship and Immigration Services (USCIS)

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

USCIS Privacy engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Built privacy into the Agile development process so that privacy is considered throughout.
- Implemented a centralized program to provide timely notification and credit monitoring services across USCIS. USCIS Privacy is responsible for providing notification to all impacted individuals whose information was or may have been breached.
- Conducted and completed 51 privacy audits (48 regional and three at Headquarters) in conjunction with extensive site visits.
- Reviewed 20 IT waivers and/or exceptions for privacy implications, and provided recommended actions to the USCIS Chief Information Officer.
- Reviewed and assessed 98 contract statements of work (SOW) to determine whether a Privacy Act Notification Clause and/or training requirements needed to be met, in accordance with the Privacy Act.

Privacy Compliance

- Achieved a FISMA score of 85 percent for PIAs and 98 percent for SORNs during this reporting period.
- Completed or updated 119 PTAs, 8 PIAs, and 1 SORN during the reporting period.

All USCIS PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

Privacy Training and Outreach

10,453 USCIS employees and contractors completed the mandatory annual online privacy awareness course.

- Sponsored privacy outreach sessions with other USCIS Directorates, facilitating a dialogue on privacy and how it is implemented at USCIS.
- Implemented a new Privacy Incident Response instructor-led training for record managers and staff to convey the requirements for reporting privacy incidents.
- Briefed program offices on privacy policies, including privacy compliance, how to safeguard PII, and the requirements for Computer Readable Extracts (CRE).
- Participated in the Data Privacy Day on January 28, 2015, in the Northeast Region.
- Implemented a Virtual Privacy Chat Room with the district offices to provide a high-level overview of privacy activities in the Federal Government and internationally.
- Published a quarterly employee newsletter, "*Privacy Chronicles*," to promote privacy awareness across USCIS.
- Trained the Forms Management Branch on privacy requirements for the forms review process.
- Instructed International Field Office Directors and Officers on how to effectively process information sharing requests from USCIS's international partners.

United States Coast Guard (USCG)

The United States Coast Guard is a branch of the armed forces of the United States, a federal law enforcement agency, a regulatory agency, a first responder and humanitarian service, and a member of the U.S. Intelligence Community. It is also the world's premier maritime service, responsible for the safety, security, and stewardship of the Nation's waters.

The USCG Privacy Office engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Collaborated with Human Resources to promulgate Commandant Instruction M12750.4A, which makes PII violations a punishable offense.
- Teamed with USCG's Office of C4 and Sensors and the Office of Public Affairs to develop a USCG mobile app for the boating public. The app provides boating safety information and enables the user to complete a float plan, request a vessel safety check, or report a navigational hazard.
- Disseminated an ISSO Bulletin with guidance on how to properly encrypt and password protect files containing PII.
- Obtained Privacy Office approval to conduct field testing on the USCG Small Unmanned Aircraft System (SUAS) at the Chesapeake Bay test range located in Webster Field, Maryland. SUAS field tests are conducted quarterly, and will evaluate each unmanned system using key performance parameters (e.g., endurance, stability, and resolution) under a wide variety of simulated but realistic operational scenarios, focusing on maritime response to situations in which human lives or marine resources are in imminent danger.
- Met monthly with USCG medical staff to improve privacy oversight and incident reporting, and enhance privacy and IT security processes in field clinics.

- Participated on the DHS UAS Working Group, contributing to a draft best practices report.
- Represented USCG on the DHS Data Framework Full Operational Capability (FOC) to deliver a baseline set of capabilities supporting the counterterrorism mission by concurrently onboarding multiple datasets, preparing for increased data hosting and throughput, promoting Department collaboration, and maturing compliance and management processes.
- Worked with NIST to vet the security of mobile devices by ensuring that adequate privacy protections are built in at the front-end of the development cycle.
- Partnered with USCG medical, records, postal and C4IT divisions to create a feasible encryption method to transfer service treatment records to NARA.
- Served as a member of USCG's Enterprise Architecture Board to ensure that privacy was embedded in the design phase of the USCG System Development Life Cycle Initiative.

Privacy Compliance

- Achieved a FISMA score of 83 percent for PIAs and 100 percent for SORNs during this reporting period.
- Completed or updated 44 PTAs, 1 PIA, and 11 SORNs during the reporting period.
- Conducted a biennial review, updated, and republished 12 SORNs in the *Federal Register*.

Highlights of privacy compliance documents:

All USCG PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

- Published a PIA Update for the Vessel Requirements for the Notice of Arrival and Departure and Automatic Identification System Rulemaking to account for the increased number of individuals whose PII is collected and stored in the Ship Arrival Notification System, and the inclusion of new data fields.

Privacy Training and Outreach

- Provided a synopsis to the USCG ISSO community describing a PTA and the interface requirements and responsibilities needed for the implementation of NIST Special Publication 800-53, Appendix J controls.
- Presented an overview of USCG Privacy at the USCG CIO Information Technology Summit, emphasizing the synergy and roles/responsibilities between privacy and the IT community, best practices for safeguarding PII, and the USCG privacy incident response protocol.

United States Customs and Border Protection (CBP)

CBP guards the Nation's borders 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.

The CBP Privacy Office (CBP Privacy) engaged in the following significant activities during this reporting period:

Privacy Policy Leadership

- Reorganized the Privacy Office under the Office of the Commissioner, and hired a CBP Privacy Officer and eight staff members to work on compliance, policy, and oversight functions.
- Led a CBP Crisis Action Team in response to a significant interagency data privacy incident that involved personnel security-related PII.
- Issued a new internal directive addressing privacy policy, compliance, and implementation.
- Issued a new internal directive designed to address the use of social media at CBP.
- Participated in the Privacy Office's PCR of CBP's use of Passenger Name Records. This PCR is discussed in detail on page 36 of this report.
- Conducted privacy reviews of new or updated procurements to determine if they required contract language to ensure vendor compliance with incident reporting, safeguarding of PII, and data management requirements.
- Participated in a feasibility study to evaluate the potential operational benefits and effectiveness of incorporating the use of Body Worn Cameras (BWC) into CBP's law enforcement operations. This BWC Feasibility Study is part of CBP's overall efforts to

increase the transparency of law enforcement encounters between CBP officers and agents and members of the public.

- Participated in an interagency conference and panel discussion on Current Technology for DNA Testing and its use for kinship verification of individuals apprehended with minors at the U.S. border. Fielded questions regarding Privacy Act and other statutory requirements with respect to the collection, retention, safeguarding, and sharing of information containing PII in a CBP system of records, based on the possible introduction and implementation of "Rapid DNA" testing.

Privacy Compliance

- Achieved a FISMA score of 56 percent for PIAs and 86 percent for SORNs during this reporting period.
- Completed or updated 62 PTAs, 6 PIAs, and 4 SORNs during the reporting period.

Highlights of privacy compliance documents:

All CBP PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

- Published a PIA for CBP's Border Surveillance Systems (BSS), a combination of surveillance systems deployed to provide comprehensive situational awareness along the United States border to assist CBP in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating U.S. law. BSS includes commercially available technologies, e.g., fixed and mobile video surveillance systems, range finders, thermal imaging devices, radar, ground sensors, and radio frequency sensors. CBP conducted this PIA because BSS collects and processes PII, including video images, photographs, radio frequency emissions, and location information.
- Published a PIA Update for the Automated Targeting System (ATS), a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based targeting scenarios and assessments. CBP published this PIA Update to describe Phase II for the Common Operating Picture program, which enhances information sharing about watchlisted travelers and their traveling companions between DHS Components.
- Published a PIA Update for the Electronic System for Travel Authorization (ESTA), a Web-based application and screening system to determine if certain foreign nationals are eligible to travel to the United States under the Visa Waiver Program. CBP published this update to provide notice of changes to the ESTA application questionnaire and expansion of the ESTA application data elements.
- Published a PIA for the 1:1 Facial Recognition Air Entry Pilot, a pilot designed to allow CBP officers stationed at air ports of entry to use facial recognition technology to assist them in determining whether an individual presenting themselves with a valid United States electronic passport is the same individual photographed in that passport. The operational goals of this pilot are to determine if facial recognition technology can be incorporated into current CBP entry processing with acceptable impacts to processing time, while effectively

providing the officers with a tool to reveal imposters. CBP issued this PIA to evaluate the privacy risks of using facial recognition software at an air port of entry.

- Published a PIA Update for the Advance Passenger Information System (APIS) to (1) provide notice of an Intelligence Community pilot leveraging APIS data shared under the terms of a Memorandum of Agreement between DHS and the National Counterterrorism Center; and (2) support the Department's mission to protect the United States from potential terrorist activities.

Privacy Training and Outreach

- Conducted privacy awareness training at the Office of Field Operations Professional Service Managers Orientation held in Washington, DC. The training covered an overview of the Privacy Act, as well as responsibilities for safeguarding PII.
- Conducted privacy awareness training for CBP Office of Field Operations supervisors at the ports of Las Vegas, Nevada, and Los Angeles, California.
- Established a new Social Media Requirements Training Course to provide an overview of privacy risks associated with the use of social media, as well as information on DHS's social media policy, including how to gain access, roles and responsibilities, and general rules of behavior for social media use.

United States Immigration and Customs Enforcement (ICE)

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

The ICE Privacy Office (ICE Privacy) engaged in the following significant activities during the reporting period:

Privacy Policy Leadership

- Led the development of an agency-wide strategy to procure access to commercially available LPR data. Co-drafted a Statement of Work that included requirements for vendors to meet strict privacy, security, and auditing protections including, but not limited to, stringent restrictions on access and use of the data. Met with Congress to explain privacy and civil liberties risk and mitigation strategies, and participated in a review of vendor proposals.

Privacy Compliance

- Achieved a FISMA score of 82 percent for PIAs and 100 percent for SORNs during this reporting period.
- Completed or updated 46 PTAs, 4 PIAs, and 4 SORNs during the reporting period.
- Responded to 33 Privacy Act amendment requests and 13 privacy complaints.
- Reviewed over 160 proposed procurements to ensure the inclusion of appropriate privacy protections in contract language.
- Reviewed for privacy compliance the ICE notice of proposed rulemaking tentatively titled *Expanding Training Opportunities for F-1 Nonimmigrant Students with Science, Technology, Engineering, or Mathematics (STEM) Degrees and Strengthening Curricular Practical Training*, providing for revisions to 8 CFR §§ 214.2, 214.3, and 274a.12.
- Resolved an estimated 84 privacy incidents, taking steps to mitigate any damages from the incidents and reduce future incidents.

- Provided advice and oversight during the development of two information sharing agreements signed during the reporting period. Assisted ICE program offices in building privacy into the framework of the agreements, and reviewed the agreements for privacy compliance.

Highlights of privacy compliance documents:

All ICE PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

- Published a PIA for FALCON-Roadrunner, a module of the larger ICE Office of Homeland Security Investigations (HSI) environment. This system generates investigative leads and conducts trend analysis to identify illicit procurement networks, terrorist groups, and hostile nations attempting to illegally obtain U.S. military products, sensitive dual-use technology, weapons of mass destruction (WMD), or chemical, biological, radiological, and nuclear materials. ICE conducted this PIA because FALCON-Roadrunner accesses and stores PII retrieved from data systems owned by DHS and other government agencies, as well as commercially and publicly available data.
- Published a PIA on the acquisition and use of LPR data from commercial services. ICE uses information obtained from LPRs as one investigatory tool in support of its criminal investigations and civil immigration enforcement actions. Because LPR information can be combined with other data to identify individuals and therefore meets the definition of PII, ICE conducted this PIA to describe how it intends to procure the services of a commercial vendor of LPR information in order to expand the availability of this information to its law enforcement personnel. In addition, through this PIA, ICE assessed the potential impact of the use of information obtained from LPRs on the civil liberties of the public, and explained the measures established to mitigate such concerns.
- Published a PIA for the National Intellectual Property Rights Coordination Center (IPR Center), an ICE-led multi-agency task force that serves as the Federal Government's clearinghouse for investigations into violations of intellectual property rights, including counterfeiting and piracy. ICE conducted this PIA because the IPR Center solicits information, including PII, through a public-facing website.
- Published a Forensic Analysis of Electronic Media PIA detailing the tools ICE uses for digital evidence examination, as well as the forensic acquisition and analysis of computer hard drives, thumb drives, cell phones, and any other data storage device obtained in the course of an investigation. ICE Homeland Security Investigations uses a variety of electronic tools to conduct criminal investigations that encompass analyzing digital media. ICE conducted this PIA because these electronic tools may be used to collect and maintain PII.
- Published an update to the Trade Transparency Analysis and Research (TTAR) SORN reflecting the replacement of its associated IT system, the Data Analysis and Research for Trade Transparency System (DARTTS), with FALCON-DARTTS, which replicates the functionality of and serves the same user groups as legacy DARTTS. The TTAR SORN was also updated to expand coverage to a new IT system launched in 2014 called FALCON-Roadrunner. As such, the SORN's categories of individuals, categories of records, records sources, and retention period for system data were modified.

- Published updates to the Immigration and Enforcement Operational Records (ENFORCE) SORN to add three new routine uses:
    - two that support ICE's sharing of information with: (1) other domestic law enforcement agencies or agencies operating sex offender registries when an alien required to register as a sex offender is released from ICE custody or removed from the United States, and (2) other government agencies or public health entities to facilitate continuity of care, and to assist with investigating and combating significant public health threats; and
    - one that supports ICE's sharing of information with domestic law enforcement agencies when an alien who has been convicted of a violent or serious crime is released from ICE custody or removed from the United States.

Privacy Training and Outreach

- Conducted new hire orientation privacy training for approximately 200 ICE Headquarters employees.
- Trained 15 public hotline operators on disclosures under the Privacy Act at the ICE Enforcement and Removal Operations Custody Programs on November 17, 2014.
- Conducted training on the operational importance of privacy, disclosures under the Privacy Act, how to safeguard PII, and privacy incidents at the ICE Homeland Security Investigations Basic Intelligence Training Course in August 2014, January 2015, and April 2015.
- Provided training on privacy and the procurement process to contracting officers, contracting officer representatives, contract specialists, program managers, and mission support staff on January 29, 2015.
- Provided training on disclosures to Congress under the Privacy Act to the ICE Office of Congressional Relations on May 19, 2015.
- Conducted a Privacy Q&A with the ICE Office of Public Affairs on June 23, 2015, to discuss the facts and effective messaging on the significant data breaches affecting federal personnel that occurred in 2014 and 2015.

United States Secret Service (USSS or Secret Service)

The Secret Service safeguards the Nation's financial infrastructure and payment systems to preserve the integrity of the economy, and protects national leaders, visiting heads of state and government, designated sites, and National Special Security Events.

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

Privacy Policy Leadership

- Engaged in USSS's Information Technology Review Committee's quarterly meetings to identify all newly proposed or operational systems, and facilitate engagements with project managers and program managers to ensure that privacy considerations are embedded in the design of each system.
- Issued an official message to all employees, reminding them of the importance of safeguarding PII, and inviting them to participate in the USSS Privacy Awareness Day.

Privacy Compliance

- Achieved a FISMA score of 100 percent for both PIAs and SORNs during this reporting period.
- Completed or updated 7 PTAs during the reporting period.

All USSS PIAs and SORNs published during the reporting period are listed in Appendix D, and can be found on the Privacy Office website: www.dhs.gov/privacy.

Privacy Training and Outreach

- Hosted a Privacy Awareness Day event entitled, "Don't Put Privacy in Jeopardy," on June 17, 2015, to educate employees and contractors about privacy best practices, federal privacy laws, and historical events related to privacy.
- Provided privacy awareness training to all new hires during biweekly orientations.
- Provided training on how to safeguard PII and report privacy incidents to all administrative officers employed at headquarters and field offices on July 23, 2014.
- Conducted privacy best practice training for special agents in charge of the investigative issues focus group on February 3, 2015.
- Created and launched a new Operational Use of Social Media Training Course to provide employees with an understanding of the specific rules of behavior to follow when using social media for law enforcement purposes.
- Distributed privacy awareness materials and posted information on privacy incidents and privacy complaints on the USSS intranet to encourage the reporting and mitigation of privacy incidents.

Appendix A – Acronym List

Acronym List	
AFI	Analytical Framework for Intelligence
AIS	Automated Indicator Sharing
App	Mobile application
ATS	Automated Targeting System
BSS	Border Surveillance Systems
BTB	Beyond the Border
CBP	United States Customs and Border Protection
CEI	Common Entity Index Prototype
CFO	Chief Financial Officer
CHCO	Chief Human Capital Office or Officer
CHWG	Cyber Hygiene Working Group
CIO	Chief Information Officer
CMA	Computer Matching Agreement
CRCL	Office for Civil Rights and Civil Liberties
CUI	Controlled Unclassified Information
CVE	Countering Violent Extremism
CVTF	Common Vetting Task Force
DARC	Data Access Request Council
DHS	Department of Homeland Security
DHS TRIP	DHS Traveler Redress Inquiry Program
DMAG	Deputy Secretary's Management Action Group
DOJ	Department of Justice
DPIAC	Data Privacy and Integrity Advisory Committee
DPPA	Data Protection and Privacy Agreement
EO	Executive Order
ESTA	Electronic System for Travel Authorization
EU	European Union
FACA	Federal Advisory Committee Act
FBI	Federal Bureau of Investigation
FCC	Five Country Conference
FEMA	Federal Emergency Management Agency
FIPPs	Fair Information Practice Principles
FISMA	Federal Information Security Management Act of 2002
FLETC	Federal Law Enforcement Training Centers
FOIA	Freedom of Information Act
FPS	Federal Protective Service
FY	Fiscal Year
GSA	General Services Administration

Acronym List	
HR	Human Resources
HSIN	Homeland Security Information Network
HQ	Headquarters
HSI	Homeland Security Investigations
I&A	Office of Intelligence and Analysis
IAPP	International Association of Privacy Professionals
IC	Intelligence Community
ICAM	Identity, Credentialing, and Access Management
ICE	United States Immigration and Customs Enforcement
IdM	Identity Management
IGA	Office of Intergovernmental Affairs
IGB	International Governance Board
IIR	Intelligence Information Report
IOC	Initial Operational Capability
ISA-IPC	Information Sharing and Access Interagency Policy Committee
ISAA	Information Sharing Access Agreement
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing Analysis Organization
ISCC	Information Sharing Coordinating Council
ISE	Information Sharing Environment
ISIL	Islamic State of Iraq and the Levant
ISP	Internet Service Provider
ISSGB	Information Sharing and Safeguarding Governance Board
ISSM	Information Security System Manager
ISSO	Information Security System Officer
IT	Information Technology
ITF	Integrated Task Force
ITP	Insider Threat Program
JRC	Joint Requirements Council
LESMC	Law Enforcement Shared Mission Community
LPR	License Plate Reader
NARA	National Archives and Records Administration
NCCIC	National Cybersecurity and Communications Integration Center
NCR	National Capital Region
NCTC	National Counterterrorism Center
NIST	National Institute of Standards and Technology
NOC	National Operations Center
NPPD	National Protection and Programs Directorate
NPRM	Notice of Proposed Rulemaking
NSTC	National Science and Technology Council
OBIM	Office of Biometric Identity Management

Acronym List	
OCIO	Office of the Chief Information Officer
OCSO	Office of the Chief Security Officer
ODNI	Office of the Director of National Intelligence
OGC	Office of the General Counsel
OGIS	Office of Government Information Services
OIG	Office of Inspector General
OIP	DOJ Office of Information Policy
OLE/FAMS	TSA Office of Law Enforcement/Federal Air Marshal Service
OMB	Office of Management and Budget
OPS	Office of Operations Coordination
PACT	Privacy Administrative Coordination Team
P/CL	Privacy and civil liberties
PCLOB	Privacy and Civil Liberties Oversight Board
PCR	Privacy Compliance Review
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIHG	Privacy Incident Handling Guidance
PLCY	Office of Policy
PNR	Passenger Name Records
PPD	Presidential Policy Directive
PPOC	Privacy Point of Contact
PRA	Paperwork Reduction Act
PTA	Privacy Threshold Analysis
RO	Reports Officer
ROMC	Reports Officer Management Council
S&T	Science and Technology Directorate
SAC	Staff Advisory Council
SAOP	Senior Agency Officials for Privacy
SBA	United States Small Business Administration
SBU	Sensitive but Unclassified
SMOUT	Social Media Operational Use Template
SOC	Security Operations Center
SORN	System of Records Notice
SOP	Standard operating procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration
UAS	Unmanned Aircraft Systems
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Services
USSS	United States Secret Service
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

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

DHS's implementation of the FIPPs is described below:[39]

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.

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

Appendix C – Compliance Activities

The Privacy Compliance Process

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

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

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

(2) the OMB IT budget submission process, which requires the Privacy Office to review all major DHS IT investments and associated systems on an annual basis, prior to submission to OMB for inclusion in the President's annual budget, to ensure that proper privacy protections and privacy documentation are in place;[40]

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

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

Privacy Compliance Documents: Keys to Transparency and Accountability

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

PTAs

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

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

PIAs

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

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

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

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

SORNs

The Privacy Act requires that federal agencies issue a SORN to provide the public notice regarding personal information 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, or other reasons. If a SORN is required, the program manager will work with the Component privacy officer or PPOC and Component counsel to write the SORN for submission to the Privacy Office. As with the PIA, the Chief Privacy Officer reviews, signs, and publishes all SORNs for the Department.

Periodic Reviews

Once the PTA, PIA, and SORN are completed, they are reviewed periodically by the Privacy Office (timing varies by document type and date approved). For systems that require only PTAs and PIAs, the process begins again three years after the document is complete or when there is an update to the program, whichever comes first. The process begins with either the update or submission of a new PTA. OMB guidance requires that SORNs be reviewed on a biennial basis.[41]

Computer Matching Agreements and the DHS Data Integrity Board

Under *The Computer Matching and Privacy Protection Act of 1988*, which amended the Privacy Act, federal agencies must establish a Data Integrity Board to oversee and approve their use of CMAs.[42] The Chief Privacy Officer serves as the Chairperson of the DHS Data Integrity Board and members include the Inspector General, the Officer for Civil Rights and Civil Liberties, the Office of the Chief Information Officer, and representatives of Components that currently have active CMA in place.[43]

Before the Department can match its data with data held by another federal agency or state government, either as the recipient or as the source of the data, it must enter into a written CMA with the other party, which must be approved by the DHS Data Integrity Board. CMAs are required when there is a comparison of two or more automated systems of records for the purpose of verifying the eligibility for cash or in-kind federal benefits.[44]

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

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

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

[43] 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).

[44] 5 U.S.C. § 552a(o).

Appendix D – Published PIAs and SORNs

Privacy Impact Assessments Published July 1, 2014 – June 30, 2015		
Component	**Name of System**	**Date Published**
CBP	DHS/CBP/PIA-001(g) Advanced Passenger Information System (APIS) ENTACT Update	6/8/2015
CBP	DHS/CBP/PIA-006(d) Automated Targeting System - TSA/CBP Common Operating Picture Program	9/23/2014
CBP	DHS/CBP/PIA-007(d) Electronic System for Travel Authorization (ESTA) PRA	11/3/2014
CBP	DHS/CBP/PIA-022 Border Surveillance Systems (BSS)	8/29/2014
CBP	DHS/CBP/PIA-025 1:1 Face ePassport Air Entry Project	3/12/2015
CBP	DHS/CBP/PIA-026 Biometric Exit Mobile (BE-Mobile) Air Test	6/19/2015
DHS-wide	DHS/ALL-027(c) Watchlist Service - IDENT	12/1/2014
DHS-wide	DHS/ALL/PIA - 032(a) Information Sharing Environment Suspicious Activity Reporting Initiative (ISE SAR)	5/13/2015
DHS-wide	DHS/ALL/PIA-038(a) Integrated Security Management System (ISMS)	9/23/2014
DHS-wide	DHS/ALL/PIA-045 Loaned Executive Program	9/30/2014
DHS-wide	DHS/ALL/PIA-046(a) DHS Data Framework Update	9/3/2014
DHS-wide	DHS/ALL/PIA-046(b) DHS Data Framework IOC Update	3/2/2015
DHS-wide	DHS/ALL/PIA-046-1(a) Neptune	9/3/2014
DHS-wide	DHS/ALL/PIA-046-1(b) Neptune IOC Update	3/2/2015
DHS-wide	DHS/ALL/PIA-046-3(a) Cerberus	9/3/2014
DHS-wide	DHS/ALL/PIA-046-3(a) Cerberus	3/2/2015
DHS-wide	DHS/ALL/PIA-047 Workman's Compensation Program – Medical Case Management Services (WC-MCMS) System	9/30/2014
DHS-wide	DHS/ALL/PIA-048(a) Foreign Access Management System (FAMS)	12/12/2014
DHS-wide	DHS/ALL/PIA-049 DHS Performance and Learning Management System (PALMS)	1/27/2015
DHS-wide	DHS/ALL/PIA-050 Enterprise Trusted Identity Exchange (TIE)	4/6/2015
DHS-wide	DHS/ALL/PIA-051 DHS Data Framework Update: Manual Transfers for an Emergent Threat	4/17/2015

Privacy Impact Assessments Published July 1, 2014 – June 30, 2015		
Component	**Name of System**	**Date Published**
FEMA	DHS/FEMA/PIA 015 Quality Assurance Recording System (QARS)	8/15/2014
FEMA	DHS/FEMA/PIA-013 Grant Management Programs REPUBLICATION	2/19/2015
FEMA	DHS/FEMA/PIA-034(a) Electronic Fingerprint System (EFS)	1/8/2015
FEMA	DHS/FEMA/PIA-039 Federal Insurance and Mitigation Administration (FIMA) Risk Insurance Division (RID) Underwriting and Claims Operation Review Tool (U-CORT)	8/29/2014
FEMA	DHS/FEMA/PIA-040 Deployment Tracking System Beta Test	3/23/2015
ICE	DHS/ICE/PIA-039 Acquisition and Use of License Plate Reader Data from a Commercial Service (LPR)	4/2/2015
ICE	DHS/ICE/PIA-040 FALCON-Roadrunner	12/1/2014
ICE	DHS/ICE/PIA-041 National Intellectual Property Rights Coordination Center	5/5/2015
ICE	DHS/ICE/PIA-042 Immigration and Customs Enforcement Forensic Analysis of Electronic Media	5/13/2015
NPPD	DHS/NPPD/PIA-020(a) Private Sector Clearance Program for Critical Infrastructure (PSCP)	2/12/2015
OPS	DHS/OPS/PIA-004(f) Publicly Available Social Media Monitoring and Situational Awareness Initiative	5/27/2015
OPS	DHS/OPS/PIA-008(d) HSIN R3 User Accounts: Identity Provider within the National Information Exchange Federation (NIEF)	9/28/2014
S&T	DHS/S&T/PIA-029 Centralized Hostile Intent (CHI)	6/10/2015
TSA	DHS/TSA/PIA-018(g) Secure Flight	1/5/2015
TSA	DHS/TSA/PIA-026(c) Alien Flight Student Program (AFSP)	7/28/2014
TSA	DHS/TSA/PIA-045 Security Threat Assessment (STA) for Conditional Access to Sensitive Security Information (SSI)	8/7/2014
USCG	DHS/USCG/PIA-006(b) Vessel Requirements for the Notice of Arrival and Departure, and Automatic Identification System Rulemaking (NOAD/AIS)	4/28/2015
USCIS	DHS/USCIS/PIA-051 Case and Activity Management for International Operations	5/27/2015

Privacy Impact Assessments Published July 1, 2014 – June 30, 2015		
Component	**Name of System**	**Date Published**
USCIS	DHS/USCIS/PIA-013-01 Fraud Detection and National Security (FDNS) Directorate	12/16/2014
USCIS	DHS/USCIS/PIA-023(a) Enterprise Citizenship and Immigration Services Centralized Operational Repository (eCISCOR)	1/23/2015
USCIS	DHS/USCIS/PIA-030(e) myE-Verify	10/6/2014
USCIS	DHS/USCIS/PIA-053 Investigations Division Case Management System	9/5/2014
USCIS	DHS/USCIS/PIA-054 National Customer Service Center (NCSC)	7/17/2014
USCIS	DHS/USCIS/PIA-055 SAS Predictive Modeling Enterprise (SAS PME)	10/15/2014
USCIS	DHS/USCIS/PIA-056 Electronic Immigration System (ELIS) Form I-90	11/14/2014

System of Records Notices Published July 1, 2014 – June 30, 2015		
Component	**Name of System**	**Date Published**
CBP	DHS/CBP-005 Advanced Passenger Information System (APIS)	3/13/2015
CBP	DHS/CBP-007 Border Crossing Information (BCI)	5/11/2015
CBP	DHS/CBP-016 Nonimmigrant Information System (NIIS)	3/13/2015
CBP	DHS/CBP-009 Electronic System for Travel Authorization (ESTA) VWP Update	11/3/2014
DHS-wide	DHS ALL-037 E-Authentication Records	8/11/2014
FEMA	DHS/FEMA-012 Suspicious Activity Reporting (SAR)	7/11/2014
FEMA	DHS/FEMA-011 Training and Exercise Programs - Biennial Update	2/23/2015
FEMA	DHS/FEMA-004 Non-Disaster Grant Management Information Files	3/13/2015
ICE	DHS/ICE-005 Trade Transparency Analysis and Research (TTAR)	12/1/2014
ICE	DHS/ICE-011 Immigration and Enforcement Operational Records (ENFORCE)	4/30/2015
ICE	DHS/ICE-011 Immigration and Enforcement Operational Records (ENFORCE),	3/2/2015
ICE	DHS/ICE-013 Alien Health Records	1/5/2015
OPS	DHS/OPS-004 Publicly Available Social Media Monitoring and Situational Awareness Initiative	5/27/2015
TSA	DHS/TSA-002 Transportation Security Threat Assessment System System of Records	8/11/2014
TSA	DHS/TSA-019 Secure Flight Records	1/5/2015
USCG	DHS /USCG-002 Employee Assistance Program Records	12/16/2014
USCG	DHS /USCG-006 Great Lakes Registered Pilot and Applicant Pilot Eligibility	12/16/2014
USCG	DHS/USCG-008 Court Martial Case Files	10/31/2014
USCG	DHS/USCG-016 Adjudication and Settlement of Claims	12/16/2014
USCG	DHS/USCG-010 Physical Disability Evaluation System Files	10/31/2014
USCG	DHS/USCG-012 Request for Remission of Indebtedness	10/31/2014
USCG	DHS/USCG-017 Federal Medical Care Recovery Act	12/16/2014
USCG	DHS/USCG-018 Exchange System and Morale Well-Being and Recreation System Files	10/31/2014
USCG	DHS/USCG-021 Appointment of Trustee or Guardian for Mentally Incompetent Personnel Files	10/31/2014
USCG	DHS/USCG-029 Notice of Arrival and Departure	10/31/2014
USCG	DHS/USCG-060 Homeport	12/16/2014
USCIS	DHS/USCIS-011 E-Verify Program	8/11/2014

Appendix E – Public Speaking Engagements

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

July 2014

- National Governor's Association's State Cybersecurity Advisory Council Virtual Meeting, Washington, DC

September 2014

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

October 2014

- Special Meeting with Privacy Advocates, Washington, DC
- *The Privacy Act 40 Years Later*, Georgetown University, Washington, DC
- Canada 2020 Conference, Privacy and Cybersecurity Panel, Ottawa, Canada

November 2014

- Privacy Summit sponsored by the CIO Council Privacy Committee, Washington, DC

December 2014

- Winter Technology Exchange sponsored by the Department of Health and Human Services, Washington, DC
- International Association of Privacy Professionals (IAPP), Practical Privacy Series – U.S. Government, Washington, DC
- Government Technology Research Alliance (GTRA) Conference, Leesburg, Virginia

January 2015

- National Reconnaissance Office's Privacy Symposium, Washington, DC
- Special Meeting with Privacy Advocates, Washington, DC

March 2015

- IAPP Global Privacy Summit, Washington, DC
- International Workshop on National Security and Societal Implications of Remotely Piloted Airborne Vehicles and Related Technologies, Washington, DC
- Federal Procurement Institute Seminar on Information Sharing, Annapolis, Maryland
- DHS FOIA Appreciation Day, Washington, DC

April 2015

- RSA Conference, San Francisco, California
- American Bar Association Spring Meeting, Washington, DC

May 2015

- FedScoop's Federal Executive Roundtable, Washington, DC
- Centre for Information Policy Leadership Retreat, Washington, DC

June 2015

- Special Meeting with Privacy Advocates, Washington, DC
- Privacy Matters Symposium: Conversations in Privacy, Department of Veteran's Affairs, Washington, DC
- Summer Technology Exchange sponsored by the Department of Health and Human Services, Bethesda, Maryland

Appendix F – Congressional Testimony and Staff Briefings

Congressional Testimony

The Chief Privacy Officer testified before the House Committee on Oversight and Government Reform on June 3, 2015 at a hearing, "Ensuring Agency Compliance with the FOIA," along with chief FOIA officers from two other agencies. The hearing examined the processes agencies use to meet FOIA's legal requirements, and explored barriers to effective and efficient compliance from the FOIA officer's perspective.

Written testimony can be found on the Privacy Office website: www.dhs.gov/privacy.

Congressional Staff Briefings

Privacy Office staff, including the Chief Privacy Officer, briefed Congress over a dozen times during the reporting period on a range of issues, including: DHS privacy policy, Privacy Office activities, data breaches, and FOIA.

Appendix G – International Outreach

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

- Financial Guard of Italy
- Carabinieri (Italy's national military police)
- Advanced School of Economy and Finance, Rome
- Italian Data Protection Authority
- Center for Internet & Society
- Cybercrime Investigation Unit, Criminal Investigation Department, Assam, India
- Viacom 18 Media, India
- Lady Shri Ram College, Delhi University
- Federation of Indian Chambers of Commerce & Industry
- Observer Research Foundation
- Totem International, Ltd.
- Digit Magazine
- Business Blogging
- Tokyo University of Technology
- Hitachi, Ltd.
- New Zealand Privacy Commissioner
- New Zealand Government Chief Privacy Officer
- National Information Society Agency, South Korea
- Engineering Academy of Armenia
- Hamburg Office for the Protection of the Constitution
- German newspaper *Thüringer Allgemeine*
- Norwegian Data Protection Authority
- Directorate General for Communications Networks, Content and Technology, European Commission