



# Department of Homeland Security

2016 Privacy Office Annual Report to Congress

*For the period July 1, 2015 – June 30, 2016*

December 12, 2016



Homeland  
Security

# Message from the Acting Chief Privacy Officer

December 12, 2016

I am pleased to present the Department of Homeland Security Privacy Office's *2016 Annual Report to Congress*, highlighting the achievements of the Privacy Office for the period July 2015 - June 2016.

I became Acting Chief Privacy Officer in July 2016 upon the departure of the Chief Privacy Officer, Karen Neuman, who led the Privacy Office for almost three years. In an interview shortly before her departure, Karen said, "Over the last decade, and specifically, over the last three years, the understanding of privacy across DHS and how it intersects with the Department's missions has increased."



"DHS Components really understand that to win and maintain the public's trust, we have to pay attention to privacy and I think that's where we've forged a very strong relationship between the Privacy Office and the professionals throughout the Components," she said. "The Privacy Office is really quite mature and the privacy enterprise reaches throughout the Department to work through embedded privacy professionals and has focused its attention on making sure that the Component leadership and others throughout the Department understand the importance of privacy as a core value, and its importance to the success of the Department's mission."

Karen stressed her pride in what the DHS privacy team accomplished during her tenure. "I think we've been extremely forward thinking and innovative in devising ways to integrate privacy protections into the Department's programs and systems. DHS, not unlike other large organizations, is using technology to assist with carrying out its various missions, and it is doing so at a time when the threat environment is very severe," she said. "We've had a lot of success, even in the current environment, in getting people to pay attention to the role that privacy plays in maintaining the public's trust and the success of DHS programs."

"I've focused on building a staff that really understands how to flip the notion of technology as invasive to a notion of technology as privacy protective. That's the overall achievement that I'm most proud of---devising really forward-thinking solutions for innovative privacy protections that avoid having to retrofit programs after the fact."

The major accomplishments of the Privacy Office this year, such as the new privacy policy for mobile applications developed by, on behalf of, or in coordination with the Department, exemplify the focus on forward-thinking solutions. More information on this, and many other accomplishments, may be found in the body of this report.

---

As we move into Fiscal Year 2017, priorities for the Privacy Office include:

- continuing to reduce the Freedom of Information Act request backlog;
- negotiating overarching Memoranda of Understanding with the Intelligence Community;
- finalizing and implementing the DHS Privacy Office Big Data and Cloud Strategy;
- working to improve privacy protections in international and/or biometric sharing agreements; and
- improving the Department's Federal Information Security Management Act (FISMA) posture to help ensure DHS systems are safe and secure.

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

Sincerely,

A handwritten signature in blue ink that reads "Jonathan R. Cantor". The signature is written in a cursive style with a large initial 'J'.

Jonathan R. Cantor  
Acting 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 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.<sup>1</sup> 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](#),<sup>2</sup> 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](#).<sup>3</sup>



To accomplish these strategic outcomes, the Privacy Office established four goals in its [Fiscal Year 2015-2018 Strategic Plan](#),<sup>4</sup> 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.

---

<sup>1</sup> 6 U.S.C. § 142.

<sup>2</sup> <http://www.dhs.gov/sites/default/files/publications/qhsr/2014-QHSR.pdf>

<sup>3</sup> <https://edit.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF>

<sup>4</sup> <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**

- Collaborated with the National Protection and Programs Directorate Office of Privacy to fulfill DHS's requirement under the Cybersecurity Information Sharing Act of 2015 to jointly issue, with the Department of Justice, interim and finalized versions of its [Privacy and Civil Liberties Guidelines](#) that govern the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with activities authorized by the Cybersecurity Information Sharing Act of 2015.<sup>5</sup>
- Partnered with the Screening and Coordination Office to: (1) renegotiate high level biometrics-based information sharing agreements with the Departments of Defense and Justice; and (2) offer advice on requirements for sharing consistent with System of Record Notices and DHS privacy policies.
- Participated in the new Social Media Task Force to assess capabilities and critical mission needs in order to identify and mitigate privacy concerns regarding current and future desired capabilities. Using social media appropriately in the context of the Department's operational missions has many potential benefits, but also presents significant risks to privacy.

### **Goal 2: Education and Outreach**

- Senior Privacy Office staff worked with the Office of Management and Budget to stand up the new Federal Privacy Council and draft its charter and by-laws. The Acting Chief Privacy Officer led a sub-committee, Privacy Talent and Career Development, which developed model privacy position descriptions, a new privacy position toolkit, and competency models for federal privacy professionals.
- In April 2016, the former Chief Privacy Officer traveled to Ottawa, Canada to discuss DHS privacy policy and the ongoing implementation of the U.S. - Canada Beyond the Border Privacy Principles in Beyond the Border information sharing projects. The Chief Privacy Officer met with numerous Canadian agencies, the Canadian Privacy Commissioner, the Business Council of Canada, and the United States Ambassador and his staff.
- Privacy Office staff continued to create and deliver a variety of ongoing and one-time privacy and transparency training courses and workshops to DHS personnel and inter-agency privacy and FOIA professionals. In addition, numerous staff spoke at conferences sponsored by prominent national associations for privacy and disclosure professionals.

### **Goal 3: Compliance and Oversight**

- Approved 57 new or updated Privacy Impact Assessments, and 18 System of Records Notices, resulting in a Department-wide Federal Information Security Management Act privacy score of 86 percent for required investment technology system Privacy Impact Assessments, and 97 percent for System of Records Notices.

---

<sup>5</sup> Cybersecurity Act of 2015, Pub. L. No. 114-113, Division N §§ 101 - 111, 129 Stat. 2242, 2942 (2015).

- 
- Completed a Framework Guidance for conducting Privacy Compliance Reviews. The Privacy Office initiates a Privacy Compliance Review at the discretion of the Chief Privacy Officer or when a Privacy Impact Assessment, System of Records Notice, or DHS agreement obligates the Privacy Office to conduct a review of a program/system to assess compliance. Under the Chief Privacy Officer's discretion, a review may be planned as part of the development of a new program or system for those programs/systems that present unique privacy concerns and/or involve controversial issues that may heighten public scrutiny.
  - Hosted a table top exercise within the Privacy Office to raise awareness of cross-team responsibilities in a breach.

#### **Goal 4: Workforce Excellence**

- Privacy Office leadership is committed to employee professional growth and development, and encourages staff to take advantage of training and development opportunities. During the reporting period, over 90 percent of staff either completed a training course or obtained certification in a job-related specialty.
- In addition, management is dedicated to mentoring students, and throughout the year partnered with several colleges and universities to provide opportunities for student internships within the Privacy Office.





# Privacy Office

## 2016 Annual Report to Congress

### Table of Contents

Message from the Acting Chief Privacy Officer.....	i
Executive Summary.....	1
Table of Contents.....	4
Legislative Language.....	6
Background.....	7
<b>I. Privacy and Disclosure Policy.....</b>	<b>11</b>
Policy Initiatives.....	12
Privacy Policy Leadership.....	13
Data Privacy and Integrity Advisory Committee.....	23
<b>II. Outreach, Education, and Reporting.....</b>	<b>24</b>
Outreach.....	25
Education: Privacy & FOIA Training and Awareness.....	28
Reporting.....	32
<b>III. Compliance and Oversight.....</b>	<b>33</b>
Privacy Compliance.....	34
FOIA Compliance.....	44
Privacy Compliance Reviews.....	41
Intelligence Product Reviews.....	44
Privacy Incident Handling.....	46
Privacy Complaint Handling and Redress.....	48

---

Privacy Act Amendment Requests .....	50
Non-Privacy Act Redress Programs .....	51
<b>IV. Workforce Excellence .....</b>	<b>52</b>
<b>V. Component Privacy Programs .....</b>	<b>54</b>
Federal Emergency Management Agency (FEMA) .....	54
National Protection and Programs Directorate (NPPD) .....	57
Office of Intelligence and Analysis (I&A) .....	61
Transportation Security Administration (TSA) .....	64
United States Citizenship and Immigration Services (USCIS) .....	67
United States Coast Guard (USCG) .....	70
United States Customs and Border Protection (CBP) .....	72
United States Immigration and Customs Enforcement (ICE) .....	75
United States Secret Service (USSS or Secret Service) .....	78
<b>Appendix A – Acronym List .....</b>	<b>80</b>
<b>Appendix B – DHS Implementation of the Fair Information Practice Principles (FIPPs) .....</b>	<b>84</b>
<b>Appendix C – Compliance Activities.....</b>	<b>85</b>
<b>Appendix D – Published PIAs and SORNs.....</b>	<b>89</b>
<b>Appendix E – Public Speaking Engagements.....</b>	<b>93</b>
<b>Appendix F – Congressional Testimony and Staff Briefings .....</b>	<b>94</b>
<b>Appendix G – International Outreach .....</b>	<b>95</b>

---

## 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 DHS Privacy Office (Privacy Office or 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, 2015, through June 30, 2016, documents the Privacy Office's continued success in safeguarding individual privacy while supporting the DHS mission.

### Statutory Framework and the Fair Information Practice Principles

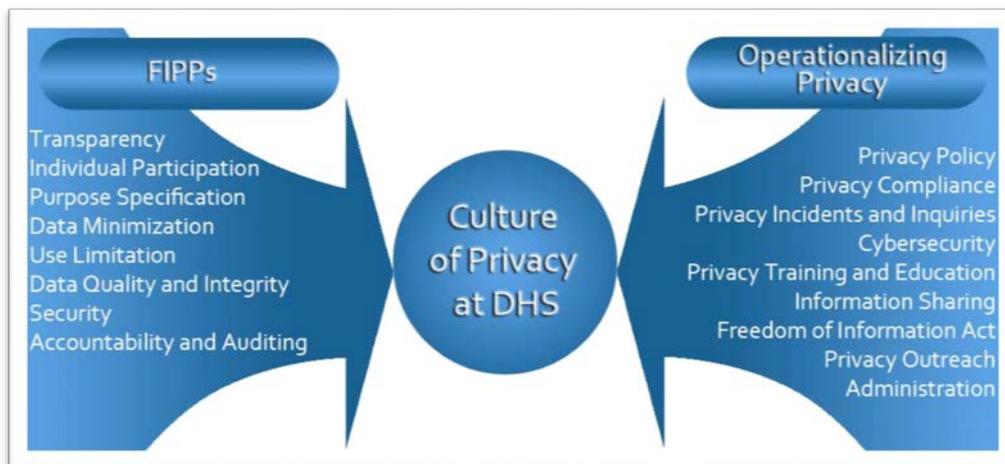
The *Homeland Security Act* charges the DHS Chief Privacy Officer with primary responsibility for ensuring that privacy considerations and protections are integrated into all DHS programs, policies, and procedures. The *Privacy Act of 1974* (Privacy Act), the *Freedom of Information Act* (FOIA), and 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 DHS Privacy Office is responsible for policy and execution of the DHS FOIA program, and meets regularly with DHS leadership to ensure continuing emphasis is placed on FOIA training, backlog reduction, closing of the agency's ten oldest requests, consultations and appeals, and ensuring that the DHS FOIA workforce has the resources required to keep the FOIA programs running efficiently to meet the President's Open Government goals.

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.<sup>6</sup>

---

<sup>6</sup> 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 (re-designated as DHS Policy Directive 140-06), *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](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf), and in DHS Management Directive 047-01, *Privacy Policy and Compliance*, July 2011, available at <https://www.dhs.gov/publication/privacy-policy-and-compliance-directive-047-01>.



*Figure 1: Privacy Office Implementation of the FIPPs*

The Privacy Office incorporates these well-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),<sup>7</sup> 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

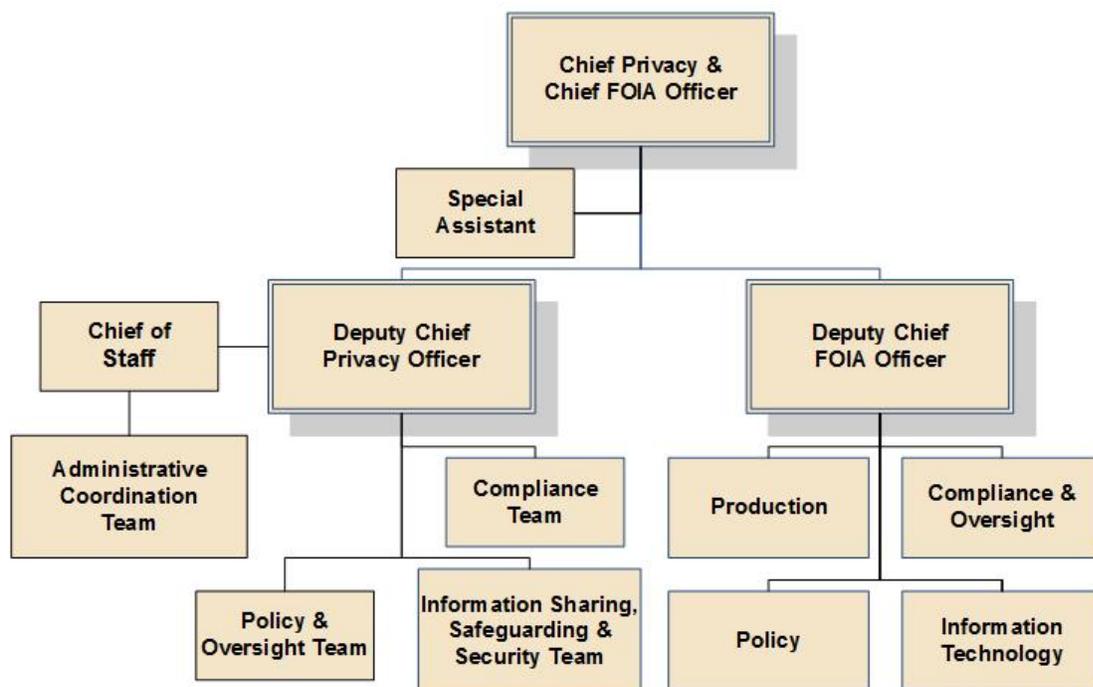
The organizational structure of the Privacy Office is aligned with, and accountable for, its four strategic goals as described in the [Privacy Office Fiscal Year \(FY\) 2015-2018 Strategic Plan](#).<sup>8</sup> Figure 2 depicts the organizational structure of the Privacy Office.

<sup>7</sup> 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.

<sup>8</sup> <http://www.dhs.gov/publication/dhs-privacy-office-strategic-plan-2015-2018>

Figure 2: Privacy Office Organizational Chart

## DHS Privacy Office



The Privacy Office is composed of five teams:

- 1) 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. In addition, this team is 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. Last, this team supports the privacy training, public outreach, and reporting functions of the Privacy Office.
- 2) 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.

- 
- 3) Information Sharing, Safeguarding, and Security 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.
  - 4) FOIA Team coordinates Department-level compliance with FOIA by developing Departmental policy to implement important FOIA initiatives, including those set forth in the President’s FOIA Memorandum and the Attorney General’s FOIA Guidelines of 2009.<sup>9</sup> Additionally, the Privacy Office coordinates and oversees Component FOIA Office operations, provides FOIA training, and prepares required annual reports on the Department’s FOIA performance. Through its FOIA team, the Privacy Office also processes initial FOIA and Privacy Act requests to the Office of the Secretary (including the Military Advisor’s Office), and many offices within DHS Headquarters.<sup>10</sup>
  - 5) 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.

---

<sup>9</sup> The President’s FOIA Memorandum of January 21, 2009, is available at: [http://www.justice.gov/oip/foia\\_guide09/presidential-foia.pdf](http://www.justice.gov/oip/foia_guide09/presidential-foia.pdf). The Attorney General’s Memorandum of March 19, 2009, is available at <http://www.usdoj.gov/ag/foia-memo-march2009.pdf>.

<sup>10</sup> In this report, a reference to the “Department” or “DHS” means the entire Department of Homeland Security, including its Components, Directorates, and the Office of the Secretary. The DHS FOIA Office processes the Privacy Office’s initial requests and those for the following 14 offices: Office of the Secretary, Office for Civil Rights and Civil Liberties, Office for Operations Coordination, Office for Community Partnerships, Office of the Citizenship and Immigration Services Ombudsman, Domestic Nuclear Detection Office, Office of the Executive Secretary, Office of Intergovernmental Affairs, Management Directorate, Office of Policy, Office of the General Counsel, Office of Health Affairs, Office of Legislative Affairs, and Office of Public Affairs.



## I. Privacy and Disclosure Policy

The Office's 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

The DHS Privacy Office has primary authority for privacy policy at the Department. During the reporting period, the Office was successful in finalizing one new privacy policy and related instruction.

### **DHS Management Instruction for DHS Mobile Applications**

Mobile applications (otherwise known as “apps”) offer numerous benefits, as they allow users to send and receive critical information in near real-time. However, these benefits can be accompanied by privacy risks that must be mitigated. These risks may include how personally identifiable information (PII), Sensitive PII, and other sensitive content such as location information, third-party data, mobile device identifiers, and metadata is collected, shared, used, and stored. Additionally, mobile apps, and the devices on which they reside, may be vulnerable to Internet security threats that may compromise a user’s information, and pose a cyber threat to the DHS systems that connect to a user’s mobile device or application.



The DHS Privacy Office strives to support the Department’s need to use state of the art technology, including mobile apps, to protect the Homeland, while protecting the privacy rights of all persons. In keeping with this mission, the Privacy Office issued a new privacy policy for mobile apps this year.

[\*Instruction 047-01-003, Privacy Policy for DHS Mobile Applications\*](#), ensures that privacy protections are built into all future and existing DHS mobile apps developed by, on behalf of, or in coordination with the Department. The policy also requires that DHS mobile apps be run through the DHS “Carwash” process, which scans the application’s code to ensure that it does not contain privacy or security vulnerabilities. To ensure that existing DHS mobile apps comply with the new policy, all DHS mobile apps that were deployed before the implementation of the policy must go through the DHS Carwash within six months of the policy’s March 30, 2016 issue date.

Since issuing the new mobile app privacy policy, the DHS Privacy Office has conducted several internal trainings to ensure that Department employees understand how to apply the policy’s unique requirements to new and existing DHS mobile apps. In addition, the DHS Privacy Office has presented this privacy policy to various members of the interagency who want to develop a privacy policy for mobile apps at their respective agencies.

Collaboration between the Privacy Office and the Office of the Chief Information Officer was critical to crafting this policy, and illustrates how privacy risks can be mitigated at the inception of a program or system, ultimately to the benefit of the Department, its workforce, and the public at large.

---

## 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.

### **DHS Biometrics Strategic Framework**

During the past year, the Privacy Office continued to support the implementation of a new DHS Biometrics Strategic Framework. Using principles set forth in the 2011 Privacy Policy Guidance Memorandum regarding Roles & Responsibilities for Shared IT Services,<sup>11</sup> the Privacy Office has supported the efforts of the Office of Policy (PLCY), Screening and Coordination Office (SCO), to promulgate a DHS Biometrics Policy. The Privacy Office also met with both Headquarters and Component stakeholders to acquaint them with proposed updates to the privacy compliance process for DHS's biometric holdings, and receive feedback to ensure a seamless integration into existing functional uses. The underlying policy considerations inform not only the manner in which biometrics will be acquired and maintained, but also how biometrics will be used and shared with DHS partners.

Following the completion of the DHS Biometrics Strategic Framework<sup>12</sup> in 2015, the Privacy Office partnered with SCO to craft a comprehensive biometrics policy, and implement an enterprise level governance structure to operationalize the concepts established by the IT Shared Services Privacy Policy. Adopting common terminology across various disciplines to define and direct stakeholder roles, such as Data Steward, Service Provider, and Data User, has helped to inform a proposed governance structure for managing the DHS Biometrics Enterprise, and has also aligned the policy decisions of that structure with existing privacy compliance documents and operational uses. This alignment across disciplines also enhances collaboration among the stakeholders, particularly between operator and oversight entities. This approach has helped to embed the oversight roles of the Privacy Office, Office for Civil Rights and Civil Liberties (CRCL), and the Office of General Counsel (OGC), which ensures the further development and execution of the strategy while continuing to protect the rights and privacy of the public.

### **Cyber Hygiene Working Group**

As explained in the 2015 Privacy Office Annual Report, the Office continues to be an active participant in the DHS Cyber Hygiene Working Group (CHWG), which includes representatives from across DHS. In March 2015, the CHWG developed two special interim clauses, Safeguarding of Sensitive Information, and Information Technology Security and Privacy Training, both of 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

---

<sup>11</sup> <http://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2011-02-roles-and-responsibilities-shared-it-services> (Privacy Policy Directive 262-09)

<sup>12</sup> [https://www.fbo.gov/index?s=opportunity&mode=form&id=eccc94e7f5bb13520a0ae392b86e9c94&tab=core&\\_cview=0](https://www.fbo.gov/index?s=opportunity&mode=form&id=eccc94e7f5bb13520a0ae392b86e9c94&tab=core&_cview=0)

---

appropriate contractor requirements for the handling of PII and Sensitive PII, along with incident reporting, breach notification, credit monitoring, and privacy training.

Since the issuance of these interim clauses, the Privacy Office has played an increased role in reviewing DHS IT acquisitions through the Information Technology Acquisition Review (ITAR) process. The ITAR process allows the Privacy Office to review DHS IT acquisitions to determine whether the acquired technology will be used to collect, maintain, access, use, or share PII, or has other privacy sensitivities associated with it, and whether the two special interim clauses need to be included within the contract or solicitation. The Privacy Office also conducted training for IT Program Managers so they may better identify PII to determine whether the special interim clauses are required in the contracts and solicitations for their respective ITARs.

The interim clauses, developed by the CHWG, will continue to ensure that sensitive information entrusted to contractors will be adequately protected while DHS completes its 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.

The CHWG also provided the Privacy Office with the ability to provide critical input during the development of several key initiatives across the Federal Government, including the Controlled Unclassified Information (CUI) Program. In September 2016, the National Archives and Records Administration, Information Security Oversight Office, issued a [Final Rule on Controlled Unclassified Information](#). The CUI Program intends to standardize the way the Executive Branch handles information that requires protection under laws, regulations, or government-wide policies, but does not qualify as classified under Executive Order 13526, Classified National Security Information, or any predecessor. The Privacy Office took part in several interagency meetings and contributed a great amount of subject matter expertise to ensure that PII would be adequately protected, commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, or dissemination, under the CUI Regulation.

### **Cybersecurity Information Sharing Act of 2015 Implementation**

On December 18, 2015, the President signed the [Cybersecurity Information Sharing Act of 2015](#) (CISA) into law.<sup>13</sup> Congress designed CISA to create a voluntary cybersecurity information sharing process that encourages public and private entities to share cyber threat information while protecting classified information, intelligence sources and methods, and privacy and civil liberties. Consistent with the requirements of CISA, DHS employs its [Automated Indicator Sharing \(AIS\) initiative](#) to



---

<sup>13</sup> Cybersecurity Act of 2015, Pub. L. No. 114-113, Division N, 129 Stat. 2242, 2942 (2015).

---

enable the timely exchange of cyber threat indicators and defensive measures among federal and non-federal entities.

The AIS initiative is an automated capability that receives, processes, and disseminates cyber threat indicators and defensive measures in real-time by enabling DHS's National Cybersecurity and Communications Integration Center (NCCIC) to: (1) receive indicators from federal and non-federal entities; (2) remove PII and other sensitive information not directly related to the cybersecurity threat; and (3) disseminate the cyber threat indicators and defensive measures, as appropriate, to other federal and non-federal entities. The National Protection and Programs Directorate (NPPD) has primary responsibility for implementing the AIS initiative, and the NPPD Office of Privacy, working in coordination with the Privacy Office, developed robust privacy protections for AIS. As a result, AIS has processes which:

- perform automated analyses and technical mitigations to delete PII that is not directly related to a cyber threat,
- incorporate elements of human review on select fields of certain indicators to ensure that automated processes are functioning appropriately,
- minimize the amount of data included in a cyber threat indicator to the information that is directly related to a cyber threat,
- retain only information needed to address cyber threats, and
- ensure that any information collected is used only for purposes authorized under CISA.

The Privacy Office also collaborated with CRCL and the NPPD Office of Privacy to fulfill DHS's requirement under CISA to jointly issue, with the Department of Justice (DOJ), interim and finalized versions of [CISA's Privacy and Civil Liberties Guidelines](#). CISA required the Attorney General and the Secretary of Homeland Security to jointly develop, submit to Congress, and make available to the public guidelines relating to privacy and civil liberties that shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with activities authorized by CISA. DHS and DOJ will continue to periodically review (no less than once every 2 years from the date of issuance) these guidelines to ensure that they are updated in accordance with statutory and policy changes, and to ensure that all privacy concerns are appropriately considered and mitigated.

### **Data Framework**

The Privacy Office continues to support the development of the DHS Data Framework, a scalable IT program that supports advanced data capabilities under formal governance processes. The Data Framework, comprised of the Neptune and Cerberus Systems, uses data tags to apply policy-based rules to determine which users can access which data for what purpose, so that 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 continued its Initial Operational Capability (IOC), which included the addition of more data sets, the operational use of the data by a controlled set of users, and planning for the addition of advanced analysis tools. The Privacy Office serves a significant role as data sets are prioritized, tagged, and moved into the Framework, and as new analysis tools are deployed.

---

## **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.

The Privacy Office supported the Joint Requirements Council (JRC), which reports to the DMAG and serves as an executive level body that provides oversight of the DHS requirements generation process, harmonizes efforts across the Department, and makes prioritized funding recommendations to the DMAG for those validated requirements. The JRC is also responsible for examining what tools and resources the Department needs in order to operate in the future across a wide variety of mission areas, including aviation fleet; screening and vetting; information sharing systems; chemical, biological, radiological, and nuclear detection; and cybersecurity. The Privacy Office provided significant support to two portfolio groups under the JRC: the Screening Portfolio and Information Sharing Portfolio Teams. These teams are responsible for evaluating various policy, resource, capability, or process issues, and providing recommendations to the JRC.

## **Information Sharing**

DHS collects a great deal of information from the general public under a variety of authorities. These authorities include benefits administration, law enforcement, intelligence, border security, and transportation security. The vast majority of the individuals in DHS systems are law abiding citizens, Lawful Permanent Residents, refugees and asylum seekers, and visitors to the United States. However, some small percentage of these individuals may intend to harm the Nation, so DHS data is extremely valuable to the entire Homeland Security Enterprise.

In light of this truth, DHS has always partnered with law enforcement, the United States Intelligence Community (IC), and even foreign governments to share information that will help identify terrorism associations and other national security concerns. In the past, however, sharing was limited largely to answering predicated queries, either by answering requests for information, or by granting account-based access to DHS systems to appropriate users.

In recent years, however, new data requests for DHS data in "bulk" have become far more routine. In bulk sharing, DHS shares entire data sets with partners, before any derogatory information is associated with any of the individual records. This carries some inherent privacy risks unique to bulk sharing, because most of the records will never be linked to derogatory information of any kind. Thus, the DHS Privacy Office had developed a number of strategies to mitigate those unique privacy risks. First, DHS is only supposed to bulk share when other, more privacy-sensitive forms of sharing, are ineffective or impracticable. When bulk sharing is the only course, DHS writes specific privacy protections into Information Sharing and Access Agreements (ISAA), such as limits to permissible users and uses, retention periods, regular audits, training provisions, understanding of the conditions that would trigger permanent retention, providing for human review of matches, reporting on use, and requiring transparency.

---

These privacy provisions mitigate the inherent privacy risks in bulk sharing. However, the Privacy Office is committed to working with agency stakeholders and DHS sharing partners to find alternatives to bulk sharing, and hone and improve the agreement provisions to provide as many protections as possible.

To further this goal, during the reporting period, the Privacy Office collaborated with Component privacy offices, the DHS Office of Intelligence and Analysis (I&A),<sup>14</sup> 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 IC.
  - As part of DHS’s Data Access Review Council (DARC), the Office incorporated privacy best practices, such as protections related to transparency, oversight, and redress into ISAAs with the IC.
  - The Privacy Office continued to participate in quarterly reviews of the National Counterterrorism Center’s (NCTC) use of DHS data, including the application of its own suite of baseline and enhanced safeguards.<sup>15</sup>
- Maintained an active leadership role in DHS’s internal information sharing and management governance processes.
  - The Privacy Office remained an active member of 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 implementation of the DHS Information Sharing and Safeguarding Strategy with the continued development of 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.
  - Through the ISCC and ISSGB, the Privacy Office supported the development of an implementing Instruction for DHS ISAAs that will establish requirements and processes for the development, execution, and cataloguing of ISAAs within the DHS Information Sharing Environment.

---

<sup>14</sup> 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.

<sup>15</sup> More information on NCTC’s data stewardship is available through its Transparency Initiative at <http://www.nctc.gov/transparency.html>.

- 
- As a member of the Executive Steering Committee for the DHS Office of Biometric Identity Management (OBIM), 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 U. S. 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 protections were in place. ATS is a 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.

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 Information Sharing Environment (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,<sup>16</sup> 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.

---

<sup>16</sup> <http://www.dhs.gov/sites/default/files/publications/12-4466-dhs-information-sharing-and-safeguarding-strategy-01-30-13--fina%20%20%20.pdf>

- 
- **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 ISE Privacy Guidelines<sup>17</sup> 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 the development of ISE Core Awareness Training and the ISE Privacy Guidelines Compliance Review Self-Assessment and Survey, which assists federal ISE agencies in assessing their continuing obligation to implement their ISE privacy protection policies and the ISE Privacy Guidelines requirements.

### **Information Sharing Through Biometric Interoperability**

The Privacy Office partnered with SCO to: (1) renegotiate high level biometrics-based information sharing agreements with the Department of Defense and DOJ; and (2) offer advice on requirements for sharing consistent with System of Record Notices and DHS privacy policies. The Privacy Office also contributed to specific information sharing projects with these agencies, providing expertise on the appropriate handling of biometric records ingested from the Department of Defense that were collected with handheld mobile devices in war zones, primarily in Iraq and Afghanistan, and assisting on a pilot project to evaluate the sharing of prints collected from individuals that U.S. military personnel encountered during Operation Enduring Freedom and Operation Iraqi Freedom. In addition, under the Texas Latent Interoperability Project, expected to commence before the end of 2016, DHS will derive mission value from Texas law enforcement agency investigative actions that establish a derogatory nexus to DHS populations (i.e., law enforcement, benefits, and travel/access privileges) by assisting with the identification of potential suspects in criminal and terrorist cases.

- **Membership in the Biometrics Institute<sup>18</sup>**

The Privacy Office joined PLCY and several Components in an annual membership in the Biometrics Institute, an independent, international organization whose mission is to promote the responsible use of biometrics. The Acting Chief Privacy Officer also addressed an audience of Biometrics Institute members on DHS's use of biometrics at its March 2016 meeting in Washington, DC.

---

<sup>17</sup> <http://ise.gov/sites/default/files/PrivacyGuidelines20061204.pdf>

<sup>18</sup> The Privacy Office submitted a review of the Biometrics Institute's draft Privacy Guidelines and its Trust Mark Proposal. The Privacy Office's input is reflected in the final Privacy Guidelines. The Trust Mark Proposal is still in draft at the time of this writing.

---

## **Insider Threat Program**

Privacy Office staff participate in the key working groups developing and implementing the DHS Insider Threat Program (ITP). Executive Order 13587<sup>19</sup> 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 of disclosing 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 operate 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](#)<sup>20</sup>, 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.

## **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 U.S.-Canada Beyond the Border Action Plan, the Five Country Conference, and Preventing and Combatting Serious Crimes Agreements.

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

- *Data Protection and Privacy Agreement.* The Chief Privacy Officer was a member of the U.S. delegation that recently signed U.S. - European Union (EU) Data Protection and Privacy Agreement (DPPA or “Umbrella” Agreement) with the European Commission. Once EU Parliamentary consent has been achieved, the DPPA will be a binding umbrella agreement for sharing law enforcement information pursuant to baseline standards for protecting PII

---

<sup>19</sup> <https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net>

<sup>20</sup> [http://dhsconnect.dhs.gov/policies/Instruction%20Supplements/262-05-002\\_Information\\_Sharing\\_and\\_Safeguarding\\_Insider\\_Threat\\_Program.pdf](http://dhsconnect.dhs.gov/policies/Instruction%20Supplements/262-05-002_Information_Sharing_and_Safeguarding_Insider_Threat_Program.pdf)

---

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, and Privacy Office staff helped provide input into 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. The Judicial Redress Act of 2015 was signed into law by the President on February 24, 2016.<sup>21</sup>

- *Mexico Statement of Cooperation.* The Privacy Office provided expertise and assisted with the drafting of a Statement of Cooperation with the Mexican National Migration Institute. The Privacy Office advised on the proof of concept for the Statement of Cooperation, a limited scope pilot of information sharing completed in advance of the Statement of Cooperation negotiation. The Statement of Cooperation contemplates use of biometric query/response to identify third-country migrants to promote the enforcement and administration of both countries' immigration laws.
- *Template Agreement On Enhancing Cooperation to Prevent Terrorist Travel and to Combat Illegal Immigration.* The Department is developing international information sharing agreements to fight against serious crime and terrorism through promoting the administration and enforcement of immigration laws. Sharing under these agreements will occur primarily through automated biometric query and response. The Privacy Office reviewed the template and, when final, will ensure that information sharing will be consistent with underlying System of Records Notices.
- *International Information Sharing Enterprise Architecture Integrated Project Team.* During the reporting period, the Office of the Chief Information Officer (CIO) and PLCY stood up an International Information Sharing Enterprise Architecture Integrated Project Team. 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 Acting Chief Privacy Officer served on the DHS International Governance Board (IGB), chaired by the Assistant Secretary for Policy. 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.

---

<sup>21</sup> Judicial Redress Act of 2015, Pub. L. No. 114-126, 130 Stat. 282 (2016), available at <https://www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf>.

---

## **Social Media Task Force**

The Department established the DHS Social Media Task Force (Task Force) to oversee, coordinate, and facilitate Department efforts towards the use of social media information in furtherance of DHS and operational Component missions. The DHS Privacy Office is a member of this task force.

Using social media appropriately in the context of the Department's operational missions has many potential benefits, but also presents significant risks to privacy. Because of this, the DHS Privacy Office is working closely with the members of the Task Force to assess capabilities and critical mission needs in order to identify and mitigate privacy concerns regarding current and future desired capabilities.

## **Unmanned Aircraft Systems: DHS Privacy, Civil Rights, and Civil Liberties Working Group on UAS<sup>22</sup>**

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 published the DHS [\*Best Practices for Protecting Privacy, Civil Rights & Civil Liberties in Unmanned Aircraft Systems Programs\*](#)



in December 2015. These best practices reflect the lessons learned through the Department's operation of UAS, and may be used by any Component whose future plans include funding or deploying UAS. They may also inform state and local law enforcement agencies about issues to consider when establishing a UAS program.

The Working Group stays informed of new developments regarding DHS's use, or possible use, of UAS, and meets routinely to discuss UAS issues, but has no immediate plans to publish additional guidance.

---

<sup>22</sup> 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>.

---

## 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.<sup>23</sup>

- On February 8, 2016, the DPIAC held a public meeting during which two members of the Privacy and Civil Liberties Oversight Board (PCLOB) gave an overview of their organization’s mission and priorities. Marc Groman, Senior Advisor for Privacy at the Office of Management and Budget (OMB), presented on the new Federal Privacy Council. [See page 26 for more information on the Council.] All four of the Privacy Office’s senior directors then reviewed their 2016 priorities. Finally, the Committee voted on and subsequently released [\*Report 2016-01 of the DHS Data Privacy and Integrity Advisory Committee on Algorithmic Analytics and Privacy Protection\*](#). This report sets forth recommendations for DHS to consider on how best to address privacy protection in the conduct of “behavioral analytics” in cybersecurity programs.
- On September 10, 2015, the DPIAC held a public meeting during which DHS briefed the Committee on privacy incidents and the new privacy policy for DHS mobile applications. A DPIAC member gave a presentation on how to protect privacy in algorithmic analytics programs. And the Chief Privacy Officer tasked the Committee to provide written guidance to the Privacy Office on best practices for notifying individuals impacted by a large-scale data breach.

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

---

<sup>23</sup> 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.

- On March 14, 2016, in Arlington, Virginia, privacy advocates met with the Chief Privacy Officer and members of the Privacy Office and NPPD Office of Privacy, and received a briefing on the implementation of the *Cybersecurity Information Sharing Act of 2015* (CISA) along with a summary of the interim Privacy and Civil Liberties Guidelines.

### Privacy and Civil Liberties Oversight Board

The Privacy Office participates in public and private meetings with the 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:

- *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 32 for more information.
- *Reports under Section 803 of the 9/11 Commission Act: Recommendations for Privacy and Civil Liberties Officers* (June 10, 2016): Privacy Office staff met with the PCLOB on several occasions to brainstorm ways to make the semiannual Section 803 Report more informative and accessible.

---

## **Federal Privacy Council (Privacy Council)**

The Federal CIO Council Privacy Committee was replaced this year with the new Federal Privacy Council, which was established by presidential [Executive Order](#) on February 9, 2016. The purpose of the new Privacy Council, which was designed to model the successful Federal CIO Council, is to help Senior Agency Officials for Privacy (SAOP) to better coordinate and collaborate, educate the federal workforce, and exchange best practices. And, like the CIO Council, the Privacy Council will develop recommendations for attracting and hiring top talent in privacy programs across the Federal Government. The Deputy Director for Management at OMB serves as the chair of the Privacy Council.



Senior Privacy Office staff worked with OMB to stand up the Privacy Council and draft its charter and by-laws. Privacy Office and Component privacy office staff support the following subcommittees:

- **Privacy Talent and Career Development:** This committee has developed model position descriptions, a new privacy position toolkit, and competency models for federal privacy professionals, and is promoting the recruitment of new talent through the Presidential Management Fellows and Pathways programs. The Acting Chief Privacy Officer co-chairs this subcommittee.
- **Education and Training:** This committee launched a monthly privacy training curriculum in 2016, and oversees a task force planning the third annual Federal Privacy Summit, to be held in November 2016.
- **Technology and Innovation:** This committee will examine privacy risks related to new technologies, and practical approaches for mitigating those risks consistent with law, guidance, policy and best practices. The Chief Privacy Officer co-chaired this committee.
- **Privacy Council Website Task Force:** The task force's objective is to develop and launch a website for the Privacy Council and the larger Federal Government privacy community under the [privacy.gov](#) domain by the end of calendar year 2016. This website will operate as a central portal with resources for the federal privacy community.

---

## **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 seven representatives from seven countries. These engagements included briefings on the U.S. privacy and FOIA frameworks, DHS privacy and disclosure policy, privacy compliance documentation, and privacy and information sharing. Privacy Office staff also briefed outgoing U.S. diplomats deployed to foreign posts, including the Deputy Chief of Mission to Ottawa.

In October 2015, the Chief Privacy Officer traveled to Amsterdam, Netherlands, to participate in the International Conference of Data Protection and Privacy Commissioners (ICDPPC). DHS holds observer status in the ICDPPC, and is granted access to closed session activities. At this year's conference, the Committee and the chairing Dutch Data Protection Authority, passed a declaration titled: *Data Protection Oversight of Security and Intelligence: The role of Data Protection Authorities in a changing society*, and adopted the *Resolution on Transparency Reporting* that was proposed by Canada and encourages the practice of 'transparency reporting' to promote accountability in relation to government access to personal information held by organizations.

In April 2016, the Chief Privacy Officer traveled to Ottawa, Canada to discuss DHS privacy policy and the ongoing implementation of the U.S. - Canada Beyond the Border (BTB) Privacy Principles in BTB information sharing projects. The meetings were scheduled at the request of PLCY to address lingering misperceptions about the U.S. privacy regime that are perceived hurdles to these deals. The Chief Privacy Officer met with numerous Canadian agencies, the Canadian Privacy Commissioner, the Business Council of Canada, and the U.S. Ambassador and his staff.

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. See Chapter V for more information on training and awareness activities sponsored by DHS Components.

### Staff Awareness

- **Political Appointees:** The Privacy Office created a factsheet for departing political appointees with instructions on how to properly secure, transfer, or destroy (consistent with records retention requirements) any PII they may have stored in paper or electronic format during their tenure.
- **Doxxing:** The Privacy Office sent all staff an email with advice on ways to protect against doxxing. Doxxing refers to gathering an individual's PII and disclosing or posting it publicly, usually for malicious purposes such as public humiliation, stalking, identity theft, or targeting an individual for harassment. Doxxers may target government employees for such purposes as identifying law enforcement or security personnel, demonstrating their hacking capabilities, or attempting to embarrass the government.

### Mandatory Online Training

Each year, DHS personnel complete the mandatory online privacy awareness training course, *Privacy at DHS: Protecting Personal Information*.<sup>24</sup> 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 and FOIA 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.

---

<sup>24</sup> This course is available on the DHS website at: [https://www.dhs.gov/xlibrary/privacy\\_training/index.htm](https://www.dhs.gov/xlibrary/privacy_training/index.htm)

- 
- **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 continued to provide privacy awareness briefings to staff throughout DHS Headquarters.



### **FOIA Training**

The DHS Privacy Office and the Component FOIA Offices conduct internal training to standardize FOIA best practices across the Department, and promote transparency and openness within DHS and among the requester community.

---

### **Classroom FOIA Training: DHS Privacy Office**

- Held a workshop for FOIA Officers and staff on the proper handling of significant FOIA requests.
- Conducted a FOIA training webinar for stakeholders of the BioWatch program.<sup>25</sup> The training included a FOIA overview tailored to a unique group, consisting of emergency first responders, local and state government offices, and the federal agencies that collaborate to carry out the BioWatch program.
- Provided a FOIA overview to the Office of the Citizenship and Immigration Services Ombudsman staff.
- Gave a half-day refresher training session to FOIA staff on how to process FOIA requests.
- Provided a two-hour FY 2015 Annual Report Refresher Training Workshop to Component FOIA staff that included reporting requirements and best practices for responding to FOIA requests.

### **Classroom FOIA Training: Component FOIA Offices**

- Transportation Security Administration (TSA) provided a two-day onsite FOIA training session with a consultant and former co-director of DOJ's Office of Information Policy (OIP), regarding FOIA exemptions and TSA-specific handling of FOIA requests.
- United States Coast Guard (USCG) legal staff conducted training for its FOIA staff on the use of exemptions.
- CBP conducted a two-day refresher training to all staff assigned to CBP FOIA headquarters. Topics included exemptions and proper application, fee waiver determinations, fee categories, and requests for expedited treatment.
- United States Citizenship and Immigration Services (USCIS) in-house training staff conducted more than 30 separate training sessions this reporting period. The training sessions were presented in a classroom setting and simultaneously for employees who were teleworking. USCIS posted several presentations on its internal website for FOIA staff.
- USCIS senior lead processors conducted refresher training sessions for all FOIA processors.
- United States Secret Service (USSS) conducted training for new Special Agents, new Uniformed Division Officers, and new employees at orientation regarding FOIA and applicable regulations. USSS also provided FOIA training to USSS Directorates and

---

<sup>25</sup> BioWatch is a cornerstone in the Department's comprehensive strategy for countering terrorism. BioWatch monitors the air for biological agents likely to be used in a bioterrorism attack. If a detection occurs, public health and other local and state officials use the information to coordinate emergency response, including prompt medical care and other actions to protect public health and safety.

---

Divisions regarding the handling of FOIA requests, search requirements, and the roles and responsibilities of the program office staff responsible for conducting searches.

- U.S. Immigrations and Customs Enforcement (ICE) conducted training during its new employee orientations, providing an overview of FOIA procedural requirements and exemptions. ICE also trained the contractors assigned to eliminate its backlog on FOIA procedural requirements, exemptions, and recent updates and changes to ICE's application of the FOIA.
- Federal Emergency Management Agency (FEMA) conducted training for its disclosure personnel to address FOIA process improvement opportunities, and to ensure consistency in processing cases. FEMA conducted additional training for its Region II, V, and VII personnel. Topics included an overview of FOIA, how to conduct records searches to yield responsive documents, timelines established within FOIA, and records management.
- I&A conducted New Employee Orientation FOIA training for both its employees and contractors. Topics included statutory requirements as well as DOJ and DHS policies. I&A conducted additional training for staff at the operational-level responsible for processing records searches and providing responsive records to I&A FOIA professionals.
- Science and Technology Directorate (S&T) conducted two annual FOIA training sessions and New Employee Orientation FOIA training for federal employees and contractors. Topics included an overview of FOIA, search requirements, and proactive disclosures.
- National Protection and Programs Directorate (NPPD) provided two, three-day FOIA training sessions to Federal Protective Service regional FOIA liaisons, as well as FOIA training to new employees and contractor support staff in its Office of Biometric Identity Management (OBIM) on the use of Exemptions 6, 7(C), 7(E), and the Privacy Act exemptions.

---

## 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 under Privacy and FOIA Reports: [www.dhs.gov/privacy](http://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,<sup>26</sup> 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*<sup>27</sup> definition of data mining.
- ***Privacy and Civil Liberties Assessment Report:*** [Executive Order 13636](https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)<sup>28</sup> (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 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.

---

<sup>26</sup> 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.

<sup>27</sup> 42 U.S.C. § 2000ee-3.

<sup>28</sup> <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.



### 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.

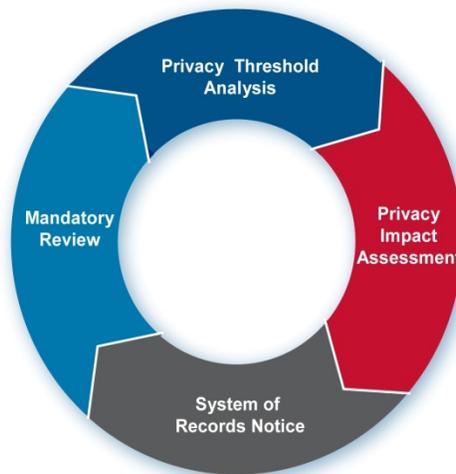


Figure 3: Privacy Office Compliance Process

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 Modernization Act of 2014* (FISMA)<sup>29</sup> 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:

---

<sup>29</sup> 44 U.S.C. § 3541.

- 
- At the end of June 2016, the Department’s FISMA privacy score showed that 86 percent of FISMA-related systems that require a PIA had a completed PIA in place, and 97 percent of required SORNs had been completed.
  - Following the release of National Institute of Standards and Technology (NIST) privacy controls for IT systems on April 30, 2013,<sup>30</sup> and further updated on January 2015,<sup>31</sup> the Compliance Team initiated a new process for reviewing and approving IT system compliance as an embedded part of the security authorization process. Since 2015, no new Authorities to Operate will be granted for IT systems without the Chief Privacy Officer’s approval.
  - 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.

**As of June 2016, the Department had a FISMA score of 86 percent for PIAs for required FISMA-related IT systems, and 97 percent for SORNs.**

---

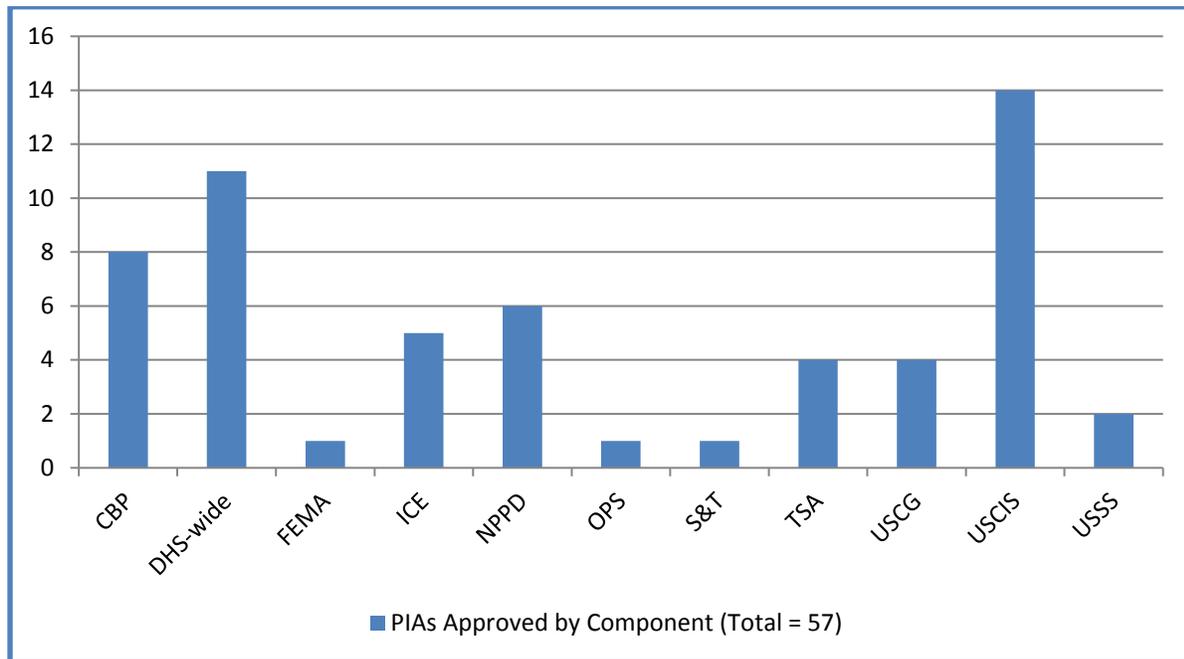
<sup>29</sup> [http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4\\_summary.pdf](http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf)

<sup>31</sup> <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

---

## **Privacy Impact Assessments**

The Privacy Office publishes new and updated PIAs on its website: [www.dhs.gov/privacy](http://www.dhs.gov/privacy). During the reporting period, the Chief Privacy Officer approved 57 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.<sup>32</sup>



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

---

<sup>32</sup> 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 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 content is being provided to Congress in a separate annex to this report.

---

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

1. [DHS/CBP/PIA-007 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 PIA to provide notice and privacy risk assessment of the updated enhancements to the ESTA application questionnaire to apply stricter screening standards to certain foreign nationals who have traveled to Somalia, Libya, and Yemen; the expansion of the ESTA application data elements in accordance with the requirements of the *Visa Waiver Program Improvement and Terrorist Travel Prevention Act of 2015*; and to include a Global Entry traveler number for ESTA applicants, if applicable. (*June 20, 2016*)

2. [DHS/CBP/PIA-027 – Southwest Border Pedestrian Exit Field Test](#)

**Background:** CBP conducted the Southwest Border Pedestrian Exit Field Test to determine if collecting biometrics (iris images and/or facial images) in conjunction with biographic data upon exit from the Otay Mesa, California land port of entry would assist CBP in matching subsequent border crossing information records with previously collected records.

**Purpose:** The purpose of the test was to evaluate whether this biometrics collection enabled CBP to identify individuals who have overstayed their lawful period of admission, identify persons of law enforcement or national security interest, and improve reporting and analysis of all travelers entering and exiting the United States. (*April 21, 2016*)

3. [DHS/FEMA/PIA-041 Operational Use of Social Media for Situational Awareness](#)

**Background:** FEMA Office of Response and Recovery launched an initiative using publicly available social media for situational awareness purposes in support of the FEMA Administrator's responsibility under the Homeland Security Act, and to assist the DHS National Operations Center (NOC) by helping to shape its mission to provide situational awareness during emergency and disaster situations in which FEMA is a primary source of information.

**Purpose:** The initiative assists FEMA's efforts to provide situational awareness for federal and international partners as well as state, local, tribal, and territorial (SLTT) governments. FEMA's Watch Centers collect information from publicly available traditional media, such as newspapers and television news, and new media sources, such as social media websites and blogs for situational awareness purposes. (*April 20, 2016*)

---

#### 4. [DHS/ALL/PIA-052 DHS Insider Threat Program](#)

**Background:** DHS Insider Threat Program (ITP) is a department-wide effort pursuant to Executive Order No. 13587 “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information<sup>33</sup>,” to protect classified national security information from unauthorized disclosure.

**Purpose:** The purpose of the ITP is to identify, detect, deter, and mitigate the unauthorized disclosure of classified information while protecting the privacy, civil rights, and civil liberties of all cleared individuals who access DHS IT systems. DHS conducted this PIA because the ITP requires access to and collection of information from data sets from multiple DHS Components, including PII associated with: (1) DHS personnel who possess security clearances granting access to classified information; (2) state, local, tribal, territorial, and private sector personnel who possess security clearances granted by DHS; and (3) any other individual who possesses a security clearance and accesses DHS IT systems or DHS classified information. *(July 13, 2015)*

#### 5. [DHS/NPPD/PIA-029 Automated Indicator Sharing](#) (See page 14 for more information.)

**Background:** NPPD Office of Cybersecurity and Communications developed an AIS initiative to enable the timely exchange of cyber threat indicators and defensive measures between the private sector and government agencies.

**Purpose:** Cyber threat indicators and defensive measures are shared consistent with the need to protect information systems from cybersecurity threats, mitigate cybersecurity threats, and comply with any other applicable provisions of law authorized by CISA for the purposes of network defense, cybersecurity, and research purposes in a manner that ensures appropriate incorporation of privacy, civil liberties, and other compliance protections. Central to the AIS initiative, the DHS National Cybersecurity and Communications Integration Center (NCCIC) serves as the centralized hub for exchanging cyber threat information indicators using a DHS-accredited infrastructure. *(March 16, 2016)*

#### 6. [DHS/NPPD/PIA-028\(a\) Enhanced Cybersecurity Services \(ECS\)](#)

**Background:** Enhanced Cybersecurity Services (ECS) is a voluntary program that shares indicators of malicious cyber activity between DHS and participating Commercial Service Providers and Operational Implementers.

**Purpose:** NPPD updated this PIA to: (1) reflect ECS’ support by Executive Order 13636, Improving Critical Infrastructure Cybersecurity; (2) announce the expansion of service beyond critical infrastructure sectors to all U.S.-based public and private entities; and (3) introduce the new Netflow Analysis Service. *(November 30, 2015)*

---

<sup>33</sup> <https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net>

---

7. [DHS/TSA/PIA-032\(d\) TSA Advanced Imaging Technology \(AIT\)](#)

**Background:** TSA deployed Advanced Imaging Technologies (AIT) for operational use to detect threat objects carried on persons entering airport sterile areas. AIT identifies potential threat objects on the body using Automatic Target Recognition software to display the location of the object on a generic figure as opposed to displaying the image of the individual.

**Purpose:** TSA updated the AIT PIA to reflect a change to the operating protocol regarding the ability of individuals to opt-out of AIT screening in favor of physical screening. While passengers may generally decline AIT screening in favor of physical screening, TSA may direct mandatory AIT screening for some passengers. *(December 18, 2015)*

8. [DHS/PIA/NPPD-027\(a\) EINSTEIN 3 – Accelerated \(E<sup>3</sup>A\)](#)

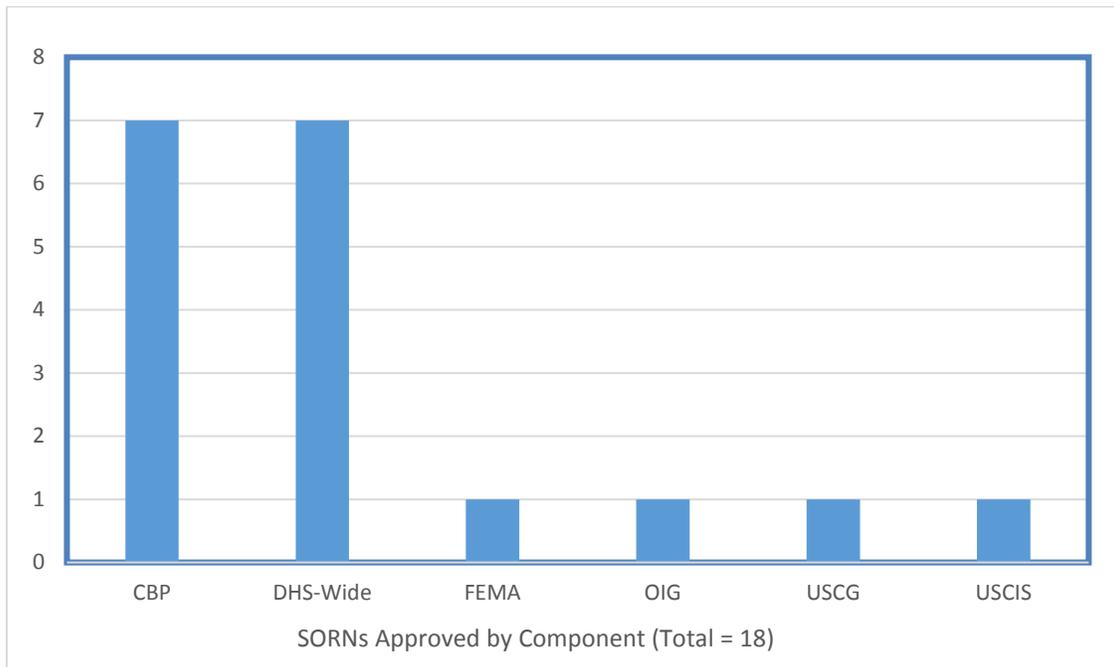
**Background:** The National Cybersecurity Protection System includes an intrusion prevention capability, operationally known as EINSTEIN 3 Accelerated (E<sup>3</sup>A), which is part of the integrated system that is used to defend the federal civilian executive branch IT infrastructure from cyber threats. With E<sup>3</sup>A, DHS is able to detect malicious traffic and take proactive measures to prevent it.

**Purpose:** NPPD conducted this PIA Update to describe the addition of a new intrusion prevention security service, known as Web Content Filtering, to the E<sup>3</sup>A program. Web Content Filtering provides protection at the application layer for web traffic by blocking access to suspicious websites, preventing malware from running on systems and networks, and detecting and blocking phishing attempts as well as malicious web content. *(May 6, 2016)*

---

## **System of Records Notices**

The Privacy Office publishes new and updated SORNs on its website: [www.dhs.gov/privacy](http://www.dhs.gov/privacy). During the reporting period, the Chief Privacy Officer approved 18 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*

---

## **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. PCRs may result in public reports or internal recommendations, depending upon the sensitivity of the program under review.

## **New Framework Guidance for PCRs**



The Privacy Office completed a Framework Guidance for conducting PCRs during the reporting period. This framework guides the design and execution of PCRs by the Privacy Office Policy and Oversight team, and can also be applied by DHS Component Privacy Offices. The Privacy Office initiates PCRs at the discretion of the Chief Privacy Officer or when a PIA, SORN or DHS agreement obligates the Office to conduct a review of a program/system to assess compliance. Under the Chief Privacy Officer's discretion, a review may be planned as part of the development of a new program or system for those programs/systems that present unique privacy concerns and/or involve controversial issues that may heighten public scrutiny.

There are eight steps in a typical PCR:

1. Collect and Review Available Background Information
2. Formulate Review Objectives
3. Notify Program of Review; Conduct Entrance Meeting
4. Formulate Review Questions and Document Requests
5. Conduct Interview(s) and Obtain Additional Supporting Documents
6. Analyze Documentation and Interviews and Draft Preliminary Conclusions
7. Review and Confirm Findings
8. Prepare and Issue Final Product

PCRs are intended to be collaborative and constructive so as to improve a program's ability to comply with assurances made in existing privacy compliance documentation. These steps provide a framework for program managers and Component Privacy Offices to look carefully at how privacy protections are actually implemented in real time. Holding programs accountable to the statements made in privacy compliance documents improves the effectiveness of the program and increases public trust in DHS operations.

---

## **PCRs Initiated or Completed During the Reporting Period**

During the reporting period, the Privacy Office completed one PCR, oversaw implementation of recommendations from two previous PCRs, assessed two self-audits of previous PCRs, and launched two new PCRs. Public PCR reports are available on the Privacy Office website: [www.dhs.gov/privacy](http://www.dhs.gov/privacy), under “Privacy Reviews and Investigations.” Each PCR listed below is hyperlinked directly to the online version.

- [Office of the Chief Human Capital Officer – Completed September 30, 2015, with ongoing oversight.](#) Following several privacy incidents, the Privacy Office conducted a PCR of the DHS Headquarters Office of the Chief Human Capital Officer (CHCO) in 2015 based on the FIPPs. The Privacy Office published its findings on September 30, 2015, which included 25 recommendations to improve the culture of privacy at CHCO. The recommendations focused on the areas of transparency/raising awareness, data minimization/retention limits, use limitations, data integrity, data security, and accountability.

Since publishing the PCR, the Chief Privacy Officer and Privacy Office staff met on multiple occasions with the Chief Human Capital Officer and CHCO staff to encourage implementation of the recommendations, focusing on steps CHCO should take to build a culture of privacy. The PCR required biannual self-audits and CHCO provided its first self-audit on March 31, 2016. However, given that human resources information is inherently privacy-sensitive, the Privacy Office expected more robust privacy practices, along with robust efforts to increase privacy awareness among its staff. The Privacy Office’s greatest concerns include high staff turnover and the lack of staff accountability. The Office continues to provide assistance and oversight, and will do so until CHCO can effectively address all 25 PCR recommendations.

- [Passenger Name Records – Completed July 2, 2015, with ongoing oversight.](#) The June 26, 2015 PCR informed discussions during the joint review of the 2011 U.S. – European Union Passenger Name Record (PNR) Agreement with the European Commission on July 1-2, 2015. This two day review included briefings from the Privacy Office, CBP, PLCY, ICE, I&A, the DHS Traveler Redress Inquiry Program, and DOJ. 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. In April 2016, the European Commission provided DHS with a draft of its conclusions from the joint review, and the Commission’s final report is expected to be published later this year.

During each month of the reporting period, the Privacy Office led PNR privacy working group meetings to monitor implementation of the PCR’s 12 recommendations, and prepare for the findings in the Commission’s report. Throughout this time, the Privacy Office found DHS stakeholders to be careful stewards of the data, faithfully following stated PNR policies and practices.

- 
- [Analytical Framework for Intelligence – Launched January 20, 2016](#). 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 from the outset to minimize privacy risks. These privacy risks are identified and discussed in the 2012 AFI PIA.

The Privacy Office required that AFI undergo a PCR within 12 months of the system’s operational deployment to assess compliance with AFI’s compliance documentation, and to ensure that the privacy protections in the PIA were being followed. On December 19, 2014, the Privacy Office made 16 recommendations to CBP to enhance AFI privacy protections, and required that a follow up PCR be completed to assess the status of the recommendations.

On January 20, 2016, the Privacy Office launched its second PCR of AFI by developing and administering a questionnaire to the AFI program that covered operations from May 2014 to March 2016. To complete this PCR, the DHS Privacy Office reviewed existing privacy compliance and usage documentation, developed an extensive questionnaire, reviewed all responses to the questionnaire, and provided follow-up questions to the AFI program office. Office staff also reviewed AFI training and governance documents and conducted site visits with, and received briefings from, AFI program personnel.

- [Media Monitoring Capability – Self audit reviewed March 14, 2016](#). PCRs are a key aspect of the layered privacy protections built into the DHS National Operations Center Media Monitoring Capability (MMC) to ensure that the protections described in relevant PIAs are followed. There have been seven PCRs led by the Privacy Office since the program began, and the MMC has consistently implemented all recommendations. As such, the May 21, 2015 PCR asked the MMC to conduct semi-annual self-assessments for the following 18 months. During this reporting period, the MMC completed an internal review on March 9, 2016. The MMC conducted follow-up actions to implement recommendations from the May 2015 PCR so as to ensure that products and processes remain consistent with the high privacy standards required by DHS. The Privacy Office found that the MMC consistently complies with privacy requirements from privacy compliance documentation.
- [Enhanced Cybersecurity Services \(ECS\) Program – Completed July 18, 2016](#). 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, based on the ECS PIA update and information provided in the [2016 Executive Order 13636 Privacy and Civil Liberties Assessment Report](#), NPPD continues to operate the ECS Program and its related processes with strong privacy oversight, which enables NPPD to identify and mitigate privacy risks as the program evolves and matures.

---

## FOIA Compliance

**FOIA requests:**<sup>34</sup> DHS continues to receive the largest number of FOIA requests of any federal department or agency in each fiscal year (FY), receiving almost 40 percent of all requests within the Federal Government.

The ever-growing volume of FOIA requests received reflects the public's interest in current events, the DHS missions, and the activities of DHS Components. CBP, ICE, OBIM, and USCIS receive the majority of FOIA requests from individuals seeking immigration related records. These Components received approximately 97 percent of all FOIA requests received by DHS in FY 2015.



**FOIA backlog:** In FY 2015, DHS received 281,138 FOIA requests and processed 348,878.<sup>35</sup> In FY 2014, DHS processed 238,003 requests. DHS closed 152,481 simple perfected requests in FY 2015, a 50 percent increase compared with the 75,687 closed in FY 2014. The Department closed 179,011 complex perfected requests in FY 2015, an 18 percent increase compared with the 146,193 closed in FY 2014. In total, DHS closed 331,492 perfected simple and complex requests in FY 2015, and released responsive records in 70 percent of those cases. This decrease is due to the joint initiatives of two Components and the DHS Privacy Office. ICE decreased its backlog by more than 99 percent, CBP decreased its backlog by 73 percent, and the DHS Privacy Office decreased its backlog by 19 percent.

The Components continued their efforts to foster a more transparent environment by proactively posting information to their websites, and engaging in practices that reduced the need for requesters to seek information through FOIA requests. A vast array of information is posted on DHS websites, including material previously available only through a formal FOIA request.

Examples include:

- historical documents;
- daily schedules of senior leaders;
- management directives;
- memoranda related to FOIA operations;
- FOIA logs;
- congressional correspondence logs;
- procurement records, including include awards, orders, and solicitations;
- purchase cardholder lists;
- FEMA disaster claims data and project worksheets;
- TSA airport throughput data;
- USCG administrative investigations;
- Office of Inspector General inspection and audit reports;

---

<sup>34</sup> For efficiency, Departmental data reflects the reporting period used in the *Freedom of Information Act Annual Report*.

<sup>35</sup> The number of requests processed includes requests received in all fiscal years.

- 
- ICE Detention Oversight Compliance Inspection Reports and list of detainee deaths while in custody;
  - USCIS records pertaining to EB-5 Regional Centers and alien files of interest;
  - S&T records pertaining to laboratory research;
  - USSS records pertaining to the Occupy movements;
  - NPPD records pertaining to new hires; and
  - CBP Juvenile Apprehension Logs and Concept of Operations Plan for Unmanned Aircraft Systems.

## 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 1,022 intelligence products and Intelligence Information Reports (IIR), 56 briefings and presentations, and 306 Requests for Information.<sup>36</sup>

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 USCIS IIRs, and found that all of them were written in a manner that adequately protected privacy.

Privacy Office staff participate in the Human Derived Intelligence Working Group (HDI-WG) (formerly known as the Reports Officer Management Council), 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 HDI-WG tackles direct dissemination of IIRs by DHS Components, and the possible need for advanced RO training. The HDI-WG is creating the training modules to grant Certified Release Authority to ROs.

---

<sup>36</sup> 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.

## Privacy Incident Handling

The Privacy Office manages privacy incident response for the Department and is the author of the *DHS Privacy Incident Handling Guidance*,<sup>37</sup> 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, 698 suspected or confirmed privacy incidents were reported to the DHS SOC, an increase of 29.5 percent from the last reporting period. Figure 6 shows the number (and percent of total) of reported DHS privacy incidents by type of incident.

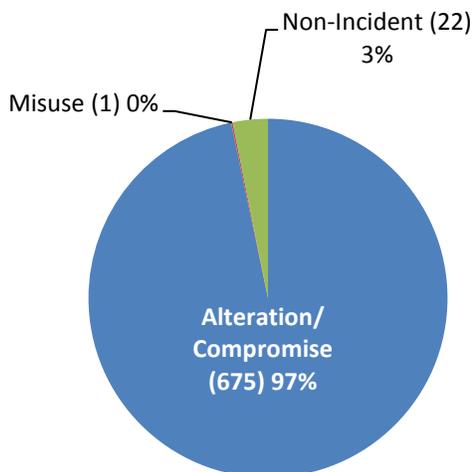
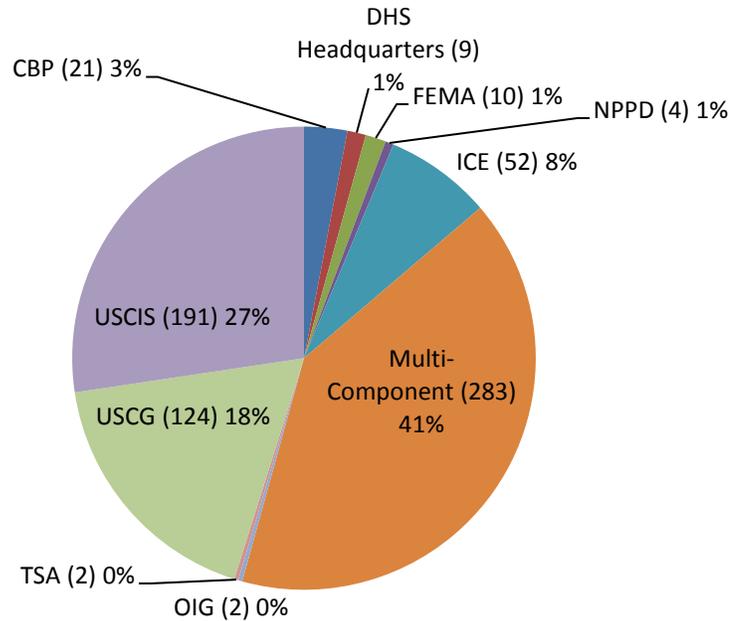


Figure 6: Percentage and Number of DHS Privacy Incidents by Type July 1, 2015 - June 30, 2016 (total = 698)<sup>38</sup>

<sup>37</sup> Available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_guide\\_pi hg.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pi hg.pdf).

<sup>38</sup> 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/>.

Figure 7 shows the number (and percent of total) of reported DHS privacy incidents by Component.



*Figure 7: Percentage and Number of DHS Privacy Incidents by Component July 1, 2015 - June 30, 2016 (total = 698)<sup>39</sup>*

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:

- participated in the Federal Incident Response Working Group supporting OMB’s efforts to update federal breach response guidance;
- hosted a table top exercise within the Privacy Office to raise awareness of cross-team responsibilities in the event of a breach;
- participated in a table top exercise hosted by the Office of the Chief Information Officer;
- developed a tip sheet for DHS personnel on ‘doxing,’ a practice in which actors post information about individuals on the Internet, usually for malicious purposes;
- developed a PIA for DHS IT security and privacy incident response activities; and
- hosted the seventh annual DHS Core Management Group Meeting in December 2015, during which stakeholders met with the Chief Privacy Officer to discuss privacy incidents and incident handling procedures.

<sup>39</sup> “Multi-Component” incidents are incidents that involve more than one DHS Component.

---

## 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.<sup>40</sup> 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, 2015 and March 31, 2016, the Department received 2,625 privacy complaints and closed 2,620. Figure 8 shows the categories and disposition of privacy complaints the Department received.<sup>41</sup>

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* (July 14, 2008)<sup>42</sup> require that the Department report semi-annually to Congress on privacy complaints received and their disposition. Chapter II of this report includes additional information on the Privacy Office's public reporting responsibilities.

---

<sup>40</sup> 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* (Privacy Policy Directive 262-12), available at [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_policyguide\\_2007-1.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf).

<sup>41</sup> 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.

<sup>42</sup> OMB Memorandum M-08-21 is available at: <http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-21.pdf>.

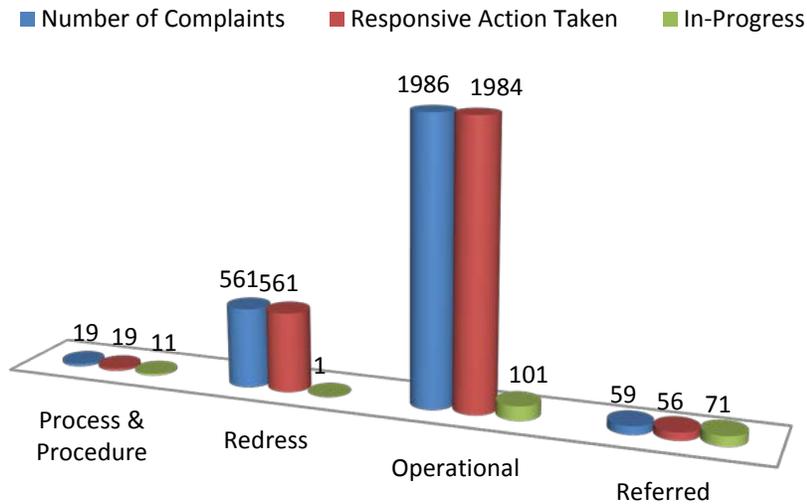


Figure 8: Privacy Complaints Received by DHS  
March 1, 2015 – March 31, 2016<sup>43</sup>

Illustrative examples of privacy complaints submitted to the Department are included in the Privacy Office’s Section 803 Reports.<sup>44</sup>

<sup>43</sup> 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.

<sup>44</sup> Available at <http://www.dhs.gov/publication/dhs-section-803-reports-congress>.

## Privacy Act Amendment Requests

The Privacy Act permits an individual to request amendment of his or her own records.<sup>45</sup> As required by *DHS Privacy Policy Guidance Memorandum 2011-01, Privacy Act Amendment Requests* (Privacy Policy Directive 140-08), 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.<sup>46</sup> 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 four DHS Components received 191 total requests.

Figure 9 shows Privacy Act Amendment Requests received by DHS during the reporting period by Component and disposition.

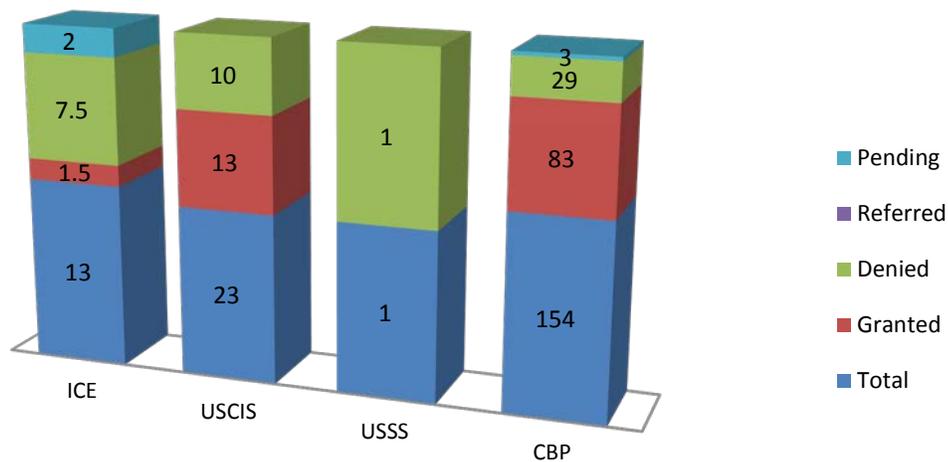


Figure 9: Privacy Act Amendment Requests by Component and Disposition  
July 1, 2015 - June 30, 2016<sup>47</sup>

<sup>45</sup> 5 U.S.C. § 552a(d)(2).

<sup>46</sup> <http://www.dhs.gov/xlibrary/assets/privacy/privacy-policy-guidance-memorandum-2011-01.pdf>.

<sup>47</sup> CBP: in 39 instances, records had already been modified or there were no other actions to take.

---

## Non-Privacy Act Redress Programs

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

- **Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP).**<sup>48</sup> DHS TRIP offers one-stop redress services to the public by providing a centralized processing point for individual travelers to submit redress inquiries. DHS TRIP was developed to assist individuals who believe they have been incorrectly denied boarding, identified for additional screening, or encounter problems at ports of entry into the country. During the reporting period July 1, 2015, through June 30, 2016, DHS TRIP received approximately 22,000 requests for redress, with an average response time (date case opened to date case closed) of approximately 46 days.
  - The Chief Privacy Officer is a member of the DHS TRIP Advisory Board. The Privacy Office Privacy also serves an active DHS TRIP practitioner. 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 109 redress requests during the reporting period.
- **Transportation Sector Threat Assessment and Credentialing Redress.** TSA's Office of Intelligence and Analysis (OIA) 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. OIA provides daily checks on over 15 million transportation sector workers against the U.S. Government's Consolidated Terrorist Watchlist. OIA 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 appeals and waivers of criminal histories.
  - During the reporting period, OIA granted 7,276 appeals and denied 282.
  - Additionally, OIA granted 2,323 waivers and denied 96.

---

<sup>48</sup> <https://www.dhs.gov/dhs-trip>



## 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.***

### Workforce

The Privacy Office continues to maintain the most dynamic, talented, and adept workforce within the federal privacy and disclosure community. The staff is consistently recognized for its expertise on substantive and emerging privacy and disclosure issues. In addition, they are often asked to provide responses to requirements and actions in support of the Department by federal, interagency, and key stakeholders. Privacy Office privacy and FOIA professionals are flexible, progressive, accomplished, and high-performing, and serve the Department with the utmost integrity and distinction to maintain public trust and achieve the Department's mission.

---

### **Staff Advisory Council - Employee Engagement**

The Staff Advisory Council (SAC) established by the Chief Privacy Officer in 2014 continues to play a significant role in strengthening employee morale, encouraging collaborative initiatives, promoting a healthy work-life balance, and fostering communication between management and staff. The SAC was formalized via charter to be an enduring source of support for Privacy Office staff, and a useful advisory body for the Chief Privacy Officer. The SAC has supported the Chief Privacy Officer in facilitating openness and transparency, and fostering a work environment that encourages teamwork and a commitment to excellence. Based on SAC recommendations from focus groups conducted with the staff, the office has implemented many new and innovative initiatives, and incorporated diversified approaches that have been beneficial and advantageous to the entire office. Privacy Office management is dedicated to implementing programs, policies, and practices that result in positive employee engagement in order to retain a resilient and motivated workforce.

### **Staff Training and Development**

Privacy Office leadership is committed to employee professional growth and development, and encourages staff to take advantage of training and development opportunities. During the reporting period, over 90 percent of staff either completed a training course or obtained certification in a job-related specialty. Numerous staff spoke at conferences sponsored by prominent national associations for privacy and disclosure professionals.

In addition, management is dedicated to mentoring students, and throughout the year partnered with several colleges and universities to provide opportunities for student internships within the Privacy Office.

---

## 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**

- Responded to two privacy-related recommendations from the June 9, 2016, DHS Office of the Inspector General (OIG) Management Advisory Report, “*FEMA Continues to Experience Challenges in Protecting Personally Identifiable Information at Disaster Recovery Centers,*” to ensure that: (1) all employees, contractors, consultants, and other FEMA personnel at disaster relief sites annually complete mandatory privacy awareness training, are aware of their responsibilities to protect and dispose of PII, and comply with privacy principles; and (2) FEMA conducts timely privacy compliance site assessments to ensure privacy protections are being implemented throughout FEMA disaster operations, to include disaster recovery centers. To comply with OIG’s recommendations, FEMA has expanded its Privacy Point of

---

Contact (PPOC) Council to appoint PPOCs for Disaster Operations. The PPOC for Disaster Operations will serve as an extension of the FEMA Privacy Office. This is being accomplished through partnership with the Office of Response and Recovery – Field Operations Directorate, and the Office of the Chief Security Officer by integrating privacy functions into the existing disaster operations functional framework for the Security Cadre who are deployed during disasters. This will ensure that at least one PPOC will be assigned to every disaster to provide privacy training, disseminate privacy resource materials, and conduct privacy compliance site assessments.

- Continued to represent privacy interests on FEMA’s Strategic Leadership Steering Committee and Integrated Project Team for FEMA’s agency-wide Workplace Transformation Initiative.
  - Provided privacy awareness training and site assessments to FEMA Program Offices within the National Capital Region (NCR).
- Represented privacy interests on the Information Governance Working Group (IGWG) on the use of DHS/FEMA SharePoint and collaboration sites. The mission of the working group is to ensure that proper privacy signage is in place to remind employees to post PII appropriately on SharePoint sites.
- Continued to report moderate to high-level privacy incidents to senior executives within the agency to establish a level of visibility into privacy incident response and mitigation, and keep senior leadership apprised of high-level incidents that could have a cross-cutting impact.
- Represented privacy and data protection interests as a permanent voting member of the FEMA Acquisition Review Board, where all decisions are made regarding FEMA’s procurements that involve PII.
- Represented privacy and data protection interests as a permanent voting member of the FEMA Data Governance Board, where all decisions are made regarding the use of the agency’s data assets that involve PII.
- Represented privacy and data protection interests as a permanent voting member of the FEMA IT Governance Board, where all decisions are made regarding the use of the agency’s IT assets that involve PII.
- Continued to serve as a permanent voting member of the FEMA Policy Working Group to ensure that all policies are developed to minimize privacy impacts.

### **Privacy Compliance**

- FISMA scores: 94 percent for PIAs and 98 percent for SORNs.
- Documents completed or updated: 57 PTAs, one PIA, and one SORN.

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](http://www.dhs.gov/privacy).

Highlights of privacy compliance documents published during this report period:

- Published a PIA on the Grant Management Program, covering 16 information collection requests and five agency IT systems.

- 
- Published a PIA update on the National Flood Insurance Program (NFIP) Information Technology Systems to support the NFIP Reinsurance Program, which will allow the sharing of flood insurance policy information to help the Federal Government reduce the amount of risk it assumes for providing flood insurance across the United States. This will be accomplished by transferring risk to reinsurance companies. This PIA update also supports the Authority to Operate (ATO) process for contractors supporting the NFIP Reinsurance Program.
  - Published a program-wide PIA for Hazard Mitigation Planning and Flood Map Products and Services Support Systems. This PIA supports three major systems and over 20 other minor SharePoint applications.
  - Published a PIA and SORN for the Operational Use of Social Media to address FEMA's use of social media to perform operations beyond communication with the public.

### **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 footprint.
- Provided a privacy briefing, along with privacy best practices and resource materials to the Field Leadership Cadre for the Missouri Floods disaster operation.
- Presented a privacy briefing at the Federal Coordinating Officers' meeting to promote a culture of privacy awareness and ensure that data protection is integrated into disaster operations.
- Continued to take proactive steps to reduce the risk of privacy breaches through dissemination of privacy reference materials and posters to highlight best practices for protecting PII and reporting and mitigating privacy incidents.

---

## 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, 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**

- Conducted two Privacy Oversight Reviews for PII handling with regards to NPPD's cybersecurity programs in November 2015 and May 2016. The focus of the reviews centered on CS&C's EINSTEIN and Cyber Information Sharing and Collaboration Program.
- Drafted and finalized privacy and civil liberties guidelines in collaboration with DOJ's Office of Privacy and Civil Liberties and the DHS Privacy Office governing the receipt, retention, use, and dissemination of cyber threat indicators by a federal entity obtained in connection with the activities authorized by CISA.
- Participated in the DHS Privacy Office assessments of NPPD activities under Executive Order 13636 and 13691.
- Developed standard operating procedures (SOP) for NPPD Office of Privacy staff conducting privacy subject matter expert (SME) reviews of NPPD contracts and statements of work.
- NPPD's Senior Privacy Officer served as co-chair of the Federal Privacy Council's E-Authentication Task Force, and members of the NPPD Office of Privacy participated in the Council's Federal Incident Response and Identity Theft Working Group, and the Contracts and Procurement Working Group.

---

## **Privacy Compliance**

- FISMA scores: 100 percent for both PIAs and SORNs.
- Documents completed or updated: 37 PTAs, six PIAs, and no SORNs.
- Conducted 201 privacy SME reviews as part of the ITAR process to ensure core privacy clauses are included 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](http://www.dhs.gov/privacy).

Highlights of privacy compliance documents published during the reporting period:

- **Automated Indicator Sharing (AIS) Initiative:** This initiative enables the timely exchange of cyber threat indicators and defensive measures among federal and non-federal entities. These cyber threat indicators and defensive measures are shared consistent with the need to protect information systems from cybersecurity threats, mitigate cybersecurity threats, and comply with any other applicable provisions of law authorized by CISA in a manner that ensures appropriate incorporation of privacy, civil liberties, and other compliance protections.
- **Chemical Facility Anti-Terrorism Standards Personnel Surety Program:** The PIA was updated to account for changes to the application, and statutory requirements of the *Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014*. The publication of the PIA update coincided with the official launch of the program.

## **Privacy Training and Outreach**

NPPD Privacy conducted the following training and awareness events:

- Hosted quarterly privacy awareness events:
  - September 2015: A panel of internal NPPD cybersecurity experts discussed the privacy risks associated with online banking, online shopping, social networking, and gaming.
  - December 2015: Annual Privacy and Technology Workshop, an interactive technology demo/fair presented by various NPPD program offices that included topics such as security, privacy, malware, encryption, and the ITAR process.
  - March 2016: Three-day *Privacy Training Days* event targeting employees and contractors in the NCR.
  - June 2016: The Privacy Officer for the Washington, DC Metropolitan Police Department presented on the privacy impact of body-worn cameras.
- All NPPD personnel completed the mandatory annual online course, *Privacy at DHS: Protecting Personal Information*.
- Provided privacy awareness briefings to all new employees at New Employee Orientation.
- Delivered Privacy Requirements for Operational Use of Social Media training to the National Infrastructure Coordinating Center.
- Provided multiple cybersecurity information handling privacy training sessions to employees and contractors in CS&C.

- 
- Provided privacy and acquisitions refresher training to a group of Contracting Officer Representatives (COR) within IP, CS&C and across NPPD lines of business. The training focused on the implementation of the Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information.
  - OBIM published one privacy tip in their internal newsletter/SharePoint website reminding employees to limit the PII they post on shared drives.
  - Provided Privacy Awareness 101 Training during an all-hands FPS Mission Support Meeting and to the FPS Personnel Security Division.
  - Provided Privacy Awareness 101 Training in Atlanta, Georgia to FPS FOIA personnel across all 11 regions.
  - The NPPD Office of Privacy relaunched its quarterly newsletter in FY 2016, entitled the *NPPD Privacy Update*. The newsletter is distributed NPPD-wide and posted on the NPPD Office of Privacy internal intranet page.

NPPD also conducted the following outreach activities:

- July 21, 2015: NPPD Senior Privacy Officer spoke on a panel entitled, “The Relationship between Privacy and Records Management,” before the Federal Records Officer Network Meeting.
- August 19, 2015: NPPD Deputy Director, Privacy, presented a briefing titled “Building Privacy Awareness” at the IRS Privacy Council.
- September 15, 2015: NPPD Deputy Director, Privacy, and an NPPD Senior Privacy Analyst spoke at an International Association of Privacy Professionals KnowledgeNet on Designing Cyber Information Sharing with Privacy in Mind.
- November 18, 2015: NPPD Senior Privacy Analyst spoke to membership of the Northern Virginia Technology Council’s Cybersecurity and Privacy Committee regarding DHS’s implementation of and the privacy protections surrounding the AIS Initiative.
- December 3, 2015: NPPD Director, Senior Privacy Officer led a session on “Identity Management Across Functional Lines,” at the 2015 Federal CIO Council Privacy Committee’s Privacy Summit.
- Between December 2015 and April 2016, NPPD Deputy Director, Privacy, and an NPPD Senior Privacy Analyst briefed the following on the development of the CISA Privacy and Civil Liberties Interim Guidelines: Federal Privacy Council members, various privacy advocacy organizations, and several federal agencies during an AIS Table Top Exercise.
- Between February 29 and March 4, 2016, NPPD Senior Privacy Officer participated on two panels entitled “Privacy Considerations in Cybersecurity Defense” and “Privacy Risk and Control Design: NIST’s Framework for Managing Privacy Risk” at the RSA conference in San Francisco, California.
- March 17, 2016: NPPD Senior Privacy Analyst participated in a panel discussion on the Perception of Privacy on Biometrics at a Biometrics Institute general membership meeting.
- May 5, 2016: NPPD Senior Privacy Officer participated in a panel discussion entitled, “Focus on Privacy Requirements and Cybersecurity,” at the DHG’s 21<sup>st</sup> Annual Government Contracting Update.

- 
- June 9, 2016: NPPD Deputy Director, Privacy, moderated a panel at the DHS CISA Public Workshop on the Privacy Considerations of CISA.

---

## 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 [Executive Order 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 Department's Social Media Task Force to examine the privacy implications of the expanded use of social media.
- Joined other privacy colleagues and IT experts in the Department's Data Framework initiative.
- Supported the Department's DARC, which coordinates the 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 the civil rights and civil liberties of the individuals whose information may be shared through those initiatives or activities.
- Participated in the Office of the Director of National Intelligence's Transparency Initiative for the Intelligence Community.

### **Privacy Compliance**

- I&A, as an element of the Intelligence Community, is exempt from FISMA reporting requirements.
- Documents completed or updated: 17 PTAs, no PIA, and no SORNs.
- Partnered with the CIO to ensure that privacy documentation is in place before any new IT investment is approved.

### **Privacy Training and Outreach**

- Provided over 50 training sessions to staff 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 safeguard 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 Policy Leadership**

- Built privacy protections into DHS social media vetting activities. DHS uses social media to vet selected groups of foreign national visa applicants to determine potential incidents of fraud.
- Worked with the Next Generation First Responder Apex Program to help tomorrow's first responder be more protected, connected, and fully aware. When firefighters, law enforcement officers, and paramedics have enhanced protection, communication, and situational awareness, they are better able to save lives. Connected data sharing involves privacy and information security risks. Building protections into new program technologies helps to limit those risks.

---

## **Privacy Compliance**

- FISMA scores: 100 percent for PIAs and 100 percent for SORNs.
- Documents completed or updated: 29 PTAs, one PIA, and no SORNs.

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](http://www.dhs.gov/privacy).

Highlights of privacy compliance documents published during this report period:

- Published a PIA for the Air Entry/Exit Re-engineering Project. The project seeks to test and evaluate various options to count the number of passengers transiting through an airport. The data will help CBP allocate staff and resources more efficiently.

---

## Transportation Security Administration (TSA)



TSA is responsible for protecting the nation's transportation systems to ensure freedom of movement for people and commerce. TSA is most visible through its airport security screening efforts at more than 450 airports, 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 more than 280 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 requests and initiatives.
- Provided advice on the expansion of TSA Pre✓<sup>®</sup> use of expanded derogatory data sets in vetting of transportation sector workers, use of social media postings in vetting of transportation sector workers, development of insider threat detection tools, disclosure of passenger information from Secure Flight to requesting law enforcement agencies, and ingest of TSA data into the DHS Data Framework for the full-range of DHS missions, including law enforcement, intelligence, and immigration.

---

## **Privacy Compliance**

- FISMA scores: 100 percent for PIAs and 100 percent for SORNs.
- Documents completed or updated: 35 PTAs, four PIAs, and no SORNs.
- 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 34 programs to validate existing privacy compliance documentation.

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](http://www.dhs.gov/privacy).

Highlights of privacy compliance documents published during the reporting period:

- **Crew Vetting Program:** TSA conducts security threat assessments on flight crew members to identify individuals who may pose a threat to transportation security. This PIA was updated to reflect that the security threat assessments will include identifying public health risks by checking crew members against the Centers for Disease Control and Prevention Do Not Board list.
- **Operations Center Incident Management System:** TSA's Transportation Security Operations Center (TSOC) serves as TSA's coordination center for transportation security incidents and operations. TSOC uses the online Emergency Operations Center incident management system to perform incident management, coordination, and situational awareness functions for all modes of transportation. TSA updated this PIA, last published on July 12, 2010, to reflect that the system receives information about individuals on watchlists and their co-travelers; logs Amber Alerts and disseminates them to the field; collects open-source information regarding transportation security or operations matters; and collects PII related to other incidents reported to TSA, including significant public health-related risks to the traveling public, and certain TSA employee information.
- **Advanced Imaging Technology:** TSA deployed Advanced Imaging Technologies (AIT) for operational use to detect threat objects carried on persons entering airport sterile areas. AIT identifies potential threat objects on the body using Automatic Target Recognition software to display the location of the object on a generic figure as opposed to displaying the image of the individual. The PIA was updated to reflect a change to the operating protocol regarding the ability of individuals to opt-out of AIT screening in favor of physical screening. While passengers may generally decline AIT screening in favor of physical screening, TSA may require AIT screening for some passengers.
- **TSA Pre✓<sup>®</sup> Application Program:** TSA operates its TSA Pre✓<sup>®</sup> Application Program to perform a security threat assessment on individuals who seek eligibility for expedited screening at participating U.S. airport security checkpoints. The PIA was updated to cover two new aspects of the program: 1) TSA will offer the ability to obtain a birth certificate certification through the National Association for Public Health Statistics and Information Systems; and 2) TSA will expand TSA Pre✓<sup>®</sup> Application Program capabilities by entering

---

into agreements with private-sector entities for marketing, enrollment, identity assurance, and criminal records checks. As part of the expansion effort, TSA will share PII collected by the program with S&T to test the ability of the private sector to perform identity assurance and criminal history assessments.

### **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, National Constitution Center, and the Computers Freedom and Privacy Conference.
- Provided privacy and privacy compliance training to TSA Business Management Officers, TSA Surface Division personnel, Paperwork Reduction Act personnel, and staff at TSA's Office of Intelligence & Analysis.
- Assisted more than 260 travelers and employees with 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**

- Provided advice and oversight to USCIS staff on the collection, maintenance, and handling of immigration data, IT security initiatives, and information sharing activities.
- Implemented a more robust Incident Management Program that requires the Regional Privacy Officers and District Privacy Officers to play an integral role in reviewing, investigating, and mitigating incidents.
- Revised the USCIS Privacy intranet site to communicate privacy information to the USCIS workforce and DHS partners.
- Reviewed Requests for Information to ensure that information sharing did not violate the FIPPs.
- Expanded the privacy footprint into additional public-facing offices for individuals seeking citizenship and benefits.
- Implemented a centralized program to provide timely notification and credit monitoring services across USCIS when deemed necessary.

- 
- Conducted and completed 51 privacy audits in conjunction with extensive site visits, using the USCIS FOIA Program, and provided recommendations on how to better integrate privacy into internal processes and procedures.
  - Reviewed and assessed 150 Statements of Work to determine whether a Privacy Act Notification Clause and/or training requirements needed to be met, in accordance with the Privacy Act.

### **Privacy Compliance**

- FISMA scores: 94 percent for PIAs and 100 percent for SORNs.
- Documents completed or updated: 181 PTAs, 14 PIAs, and one SORN.

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](http://www.dhs.gov/privacy).

### **Privacy Training and Outreach**

16,695 USCIS employees and contractors completed the mandatory annual online privacy awareness course.

- Trained 75 employees on privacy requirements for the operational use of social media.
- Published a quarterly newsletter, “*Privacy Chronicles*,” which provides guidance on privacy policies, privacy compliance requirements, privacy incident requirements, privacy complaints, privacy training, and upcoming privacy trainings and events.
- Developed a process for reviewing and determining high risk contracts to comply with the new guidance issued March 9, 2015, Class Deviation 15-01, from the Homeland Security Acquisitions Regulations: Safeguarding of Sensitive Information.<sup>49</sup> This new process ensures that all contracts are reviewed to determine if sensitive information will be a requirement of the contract. If so, stakeholders must review and comply with the high risk determination. The USCIS Office of Privacy makes the initial determination for all potential high risk contracts.
- Published a bi-annual thank you letter from the Chief Privacy Officer to USCIS leadership, thanking them for promoting a culture of privacy throughout the agency.
- Published quarterly memos to all USCIS personnel regarding their role as privacy data stewards. Topics included *USCIS’ Commitment to Protecting PII and Promoting a Culture of Privacy*, dated January 14, 2016, reminding USCIS personnel of their responsibility to protect PII and Sensitive SPII, and *Reporting Privacy Incidents*, dated May 2, 2016, with emphasis on understanding, recognizing, and reporting privacy incidents.
- Hosted the fifth annual USCIS Privacy Awareness Day on September 2, 2015. The theme was *Privacy-How to Protect Information*, and focused on how to mitigate a data breach.
- Conducted the following privacy briefings and trainings: Mandatory Privacy Awareness Training; Privacy Incident Management Requirements; Privacy Act Training; Information Sharing Training; IT acquisition and development activities; Identity Theft during Tax Season and how to protect your information; Privacy Compliance Overview of the Internal

---

<sup>49</sup> <https://www.dhs.gov/sites/default/files/publications/HSAR%20Class%20Deviation%2015-01%20Safeguarding%20of%20Sensitive%20Information.pdf>

---

Form Process; Office of Personnel Management data breaches to USCIS employees and leadership; and Privacy Requirements for the Operational Use of Social Media 1.0.

- Published and disseminated four privacy awareness posters throughout USCIS facilities. Three of the posters were internal-facing posters on protecting PII and Sensitive PII, storing and securing official records, and reporting privacy incidents. USCIS also published a bilingual public-facing poster to promote USCIS' commitment to protecting the public's personal information, which provided a point of contact for privacy-related concerns.
- Instructed International Field Office Directors and Officers on how to effectively process information sharing requests from USCIS' international partners.

---

## United States Coast Guard (USCG)



The United States Coast Guard is the world's premier, multi-mission, maritime service, responsible for the safety, security, and stewardship of the Nation's waters. The Coast Guard employs its broad authorities, expansive network of interagency, military, industry relationships, unique operational capabilities, and international partnerships to execute daily, steady-state operations, and respond to major incidents.

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

### **Privacy Policy Leadership**

- Collaborated with Coast Guard Cyber Command to outline procedures for privacy incident response and privacy compliance documentation in the Information System Security Officer Desktop Reference Guide.
- Partnered with USCG Health Insurance Portability and Accountability Act representative to issue a notice advising all personnel that PII must be destroyed using a cross-cut shredder rather than burn bags.
- Partnered with numerous USCG programs and submitted Interconnection Security Agreements and a PTA to the DHS Geospatial Management Office for Maritime Global Awareness Network and Enterprise Geographic Information System data to be utilized in the Joint Task Force Southern Border and Approaches Campaign.
- Collaborated with USCG's Office of C4 and Sensors and launched the Incident Management Handbook mobile app. This app provides Incident Command System forms and templates that can be used by first responders at the federal, state, and local levels during a major mishap or catastrophic event.

- 
- Responded to the Department of Defense PII Repository Hardening data call and identified a privacy system in the USCG CIO's inventory.

### **Privacy Compliance**

- FISMA scores: 86 percent for PIAs and 98 percent for SORNs.
- Documents completed or updated: 82 PTAs, four PIAs, and one SORN.
- Reviewed directives, forms, and information collection as a part of the clearance process, which resulted in additional Privacy Act statements, submission of compliance documentation, etc., to ensure adherence to current federal privacy mandates.

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](http://www.dhs.gov/privacy).

Highlights of privacy compliance documents published during the reporting period:

- Published a PIA update for the Transportation Worker Identification Credential Reader Requirements for U.S. Coast Guard. This PIA requires owners or operators whose vessel or facilities meet a certain risk analysis threshold to conduct an electronic inspection whenever a person is granted unescorted access to a secure area.
- Published a PIA on Rescue 21, USCG's advanced command, control, and direction-finding communications system used during search and rescue operations.
- Published Coast Guard Maritime Information Exchange PIA. This system provides maritime information to the public, and facilitates information sharing with federal, state, and local governments.

### **Privacy Training and Outreach**

- USCG Privacy and the Assistant Commandant for Intelligence provided an overview of intelligence activities and the interface with privacy to the Privacy and Civil Liberties Oversight Board.
- Presented an overview of USCG Privacy at the annual USCG CIO C4ISR&IT Strategic Summit, which emphasized the synergy between privacy and the IT community, and provided tips on safeguarding PII along with a privacy incident response protocol.

---

## U.S. 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**

- Hired additional staff to work on privacy compliance, policy, and oversight functions.
- Revised the sign-on process for the TECS system to eliminate the use of Social Security numbers. With the modernization of the TECS system, CBP users are able to log in using their DHS-CBP issued Personal Identity Verification (PIV) card.
- Finalized the CBP Crisis Team After Action Report in response to a significant interagency data privacy incident that involved personnel security-related PII. The After Action report provided lessons-learned and recommendations, and was forwarded to the CBP Office of the Commissioner for final action.
- Led CBP’s participation in the U.S. – EU Joint Review of the PNR Agreement.
- Presented a briefing on CBP Privacy during the September 2015 meeting of the Data Privacy and Integrity Advisory Committee.
- 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.

---

## **Privacy Compliance**

- FISMA scores: 63 percent for PIAs and 91 percent for SORNs.
- Documents completed or updated: 67 PTAs, eight PIAs, and seven SORNs.

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](http://www.dhs.gov/privacy).

Highlights of privacy compliance documents published during the reporting period:

- **Automated Commercial Environment (ACE):** ACE is the backbone of CBP’s trade information processing and risk management activities, and the key to implementing many of the agency’s trade transformation initiatives. ACE allows efficient facilitation of imports and exports, and serves as the primary system used by U.S. Government agencies to process cargo. ACE serves as the “Single Window” for trade facilitation, as mandated by Executive Order 13659, *Streamlining the Export/Import Process for America’s Businesses*. CBP published this PIA because ACE collects, maintains, uses, and disseminates import and export information from the trade community that contains PII.
- **Southwest Border Pedestrian Exit Field Test:** CBP conducted the Southwest Border Pedestrian Exit Field Test to determine if collecting biometrics (iris images and/or facial images) in conjunction with biographic data upon exit from the Otay Mesa, California land port of entry will assist CBP in matching subsequent border crossing information records with previously collected records. The purpose of the test was to evaluate whether this biometrics collection will enable CBP to identify individuals who have overstayed their lawful period of admission, identify persons of law enforcement or national security interest, and improve reporting and analysis of all travelers entering and exiting the United States. CBP conducted this PIA because this test collected PII from members of the public.
- **1:1 Facial Comparison Project:** CBP is expanding the 1-to-1 Facial Comparison Project (previously called the “1:1 Facial Air Entry Pilot”) to operations in all U.S. air ports of entry, and expanding the in-scope population to first-time travelers from Visa Waiver Program countries. The use of facial comparison technology assists CBP Officers in determining whether an individual presenting a valid electronic passport (e-Passport) is the individual pictured on the passport. CBP updated this PIA because the 1-to-1 Facial Comparison Project collects PII in the form of facial images of travelers to assist CBP Officers in making admissibility determinations.

---

## **Privacy Training and Outreach**

- Held four privacy awareness training sessions as part of audit refresher training for the Office of Field Operations. The sessions included an overview of the Privacy Act, as well as responsibilities for handling and safeguarding PII.
- Led six privacy training sessions over three days in Laredo, Texas; attendees included all CBP operational Components as well as attendees from ICE. The training sessions incorporated all aspects of privacy, including compliance with the Privacy Act, handling PII, reporting PII incidents, information sharing, and the operational use of social media. The trainings included real-life case studies, enabling the attendees to better understand how privacy impacts their work.
- Provided privacy training to Component offices' Privacy Liaisons who serve as the point of contact and initial identifier of privacy issues on behalf of their operational Component or program office.
- Initiated a series of privacy-related email messages to all CBP staff.
- Included privacy-related messages on two payroll statements; the messages included information on how to contact the Privacy Office with questions or concerns.
- Collaborated with CBP's Office of Information and Technology to update its *2016 IT Computer Security Awareness and Rules of Behavior Training* with information on privacy awareness.
- Presented on how to mitigate and remedy privacy incidents at the American Society of Access Professionals National Training Conference.
- Conducted PIA and SORN training for over 25 Office of Information and Technology staff.

---

## 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**

Established the Information Governance and Privacy Office (IGP), which consolidates the Privacy, Records Management, and Information Governance offices into a single organization. IGP oversees the management, sharing, protection, and access to ICE data, and ensures the information ICE maintains meets all legal and policy requirements. The Office's mission is to ensure the integrity and usability of the agency's records and data, and that individual privacy is protected.

### **Privacy Compliance**

- FISMA scores: 92 percent for PIAs and 100 percent for SORNs.
- Documents completed or updated: 57 PTAs, five PIAs, and no SORNs.
- Responded to 17 Privacy Act amendment requests and 9 privacy complaints.
- Reviewed over 160 proposed procurements to ensure the inclusion of appropriate privacy protections in contract language.
- Provided advice and oversight during the development of 20 information sharing agreements signed during the reporting period.
- Resolved an estimated 102 privacy incidents, taking steps to mitigate any damages from the incidents and reduce future incidents.

---

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](http://www.dhs.gov/privacy).

Highlights of privacy compliance documents published during the reporting period:

- **Published a PIA on SharePoint Matter Tracking Systems:** These systems track, manage, review, and report on matters related to law enforcement and non-law enforcement activities. ICE conducted this PIA to assess the privacy risks of SharePoint as a tracking tool.
- **Published a PIA on the Investigative Case Management system:** This system replaced ICE's use of the case management module in Legacy TECS, and serves as the core law enforcement case management tool primarily used by ICE Homeland Security Investigations (HSI) special agents and personnel.
- **Published a PIA on the LeadTrac System:** LeadTrac is a database owned by the ICE Counterterrorism and Criminal Exploitation Unit. The system vets and manages leads pertaining to visitors to the United States who are suspected of overstaying their period of admission or otherwise violating the terms of their admission, as well as organizations suspected of immigration violations.
- **Published two PIA updates for the Enforcement Integrated Database:** The updates include the integration of the Law Enforcement Notification System and the Criminal History Information Sharing Program. The Law Enforcement Notification System update accounts for a new messaging capability within the database that pulls existing data on aliens who have been convicted of a violent or serious crime and released from ICE custody, and creates a notification message to other law enforcement agencies. The Criminal History Information Sharing Program update describes a change to the program whereby ICE will use a secure web service to share criminal history information with its foreign partners.

### **Privacy Training and Outreach**

- Conducted new hire orientation privacy training for approximately 200 ICE Headquarters employees.
- Gave the keynote address at the International Association of Privacy Professionals Practical Privacy Series on November 18, 2015.
- Participated in a panel discussion on *How to Report a Privacy Incident* at the U.S. Department of Veterans Affairs on January 28, 2016.
- Presented on ICE Privacy's role in the acquisitions process to the ICE Acquisitions Community of Practice on March 17, 2016.
- Participated in a panel discussion on *Re-working Privacy Management within the Federal Government* at the International Association of Privacy Professionals Privacy Global Summit on April 6, 2016.
- Provided agency-wide guidance on how ICE employees and contractors can reduce their chances of identity theft and identity fraud by establishing a *Protecting Your Identity* intranet portal.

- 
- Trained seven Information Disclosure Unit employees on general privacy concepts and disclosure scenarios under the Privacy Act at the ICE Enforcement and Removal Operations Information Disclosure Unit on October 27, 2015.
  - Provided training on general privacy concepts and disclosure scenarios under the Privacy Act and FOIA for approximately 20 ICE FOIA employees on February 23, 2016.

---

## 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**

- Participated in a PII working group established by the USSS Director to assess the use, collection, maintenance, and safeguarding of PII.
- Issued an official message to all employees to remind them of the Secret Service privacy policy, which established rules of behavior for the use of social media for both law enforcement and non-law enforcement purposes, and mandated an annual training requirement for the Operational Use of Social Media.
- Updating the USSS Privacy Act directive.
- Created a new directive to provide guidance for the proper handling and safeguarding of PII and Sensitive PII.

---

### **Privacy Compliance**

- FISMA scores: 67 percent for PIAs and 91 percent for SORNs.
- Documents completed or updated: eight PTAs, two PIAs, and no SORNs.
- Reviewed and drafted Privacy Act statements for new and existing USSS forms.

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](http://www.dhs.gov/privacy).

### **Privacy Incident Response and Mitigation**

Issued an official message to all USSS employees on the importance of safeguarding PII and reporting privacy incidents, reminding employees of the dedicated phone line and e-mail address for privacy-related incidents, inquires, and/or comments.

### **Privacy Training and Outreach**

- Hosted a Privacy Awareness Day event entitled, “Spin the Privacy Wheel,” on June 22, 2016, to educate employees and contractors about privacy best practices, federal policy laws, and historical events related to privacy.
- Disseminated posters and flyers with tips on how to safeguard PII in an effort to promote privacy awareness.
- Continued to update the USSS intranet page to disseminate information to employees about privacy, compliance, guidelines, and tools.
- Provided mandatory online privacy awareness training all employees and contractors.
- Provided mandatory training on the Operational Use of Social Media to employees whose positions require it.
- Instituted a formal instructor-led privacy training class for new Special Agents and Uniformed Division Officer recruits.
- Provided privacy training at bi-weekly new employee orientation classes.
- Created a bookmark informing individuals of ways to safeguard PII.

## Appendix A – Acronym List

Acronym List	
<b>ACE</b>	Automated Commercial Environment
<b>AFI</b>	Analytical Framework for Intelligence
<b>AIS</b>	Automated Indicator Sharing
<b>AIT</b>	Advanced Imaging Technology
<b>App</b>	Mobile application
<b>ATO</b>	Authority to Operate
<b>ATS</b>	Automated Targeting System
<b>BSS</b>	Border Surveillance Systems
<b>BTB</b>	Beyond the Border
<b>CBP</b>	U.S. Customs and Border Protection
<b>CEI</b>	Common Entity Index Prototype
<b>CFO</b>	Chief Financial Officer
<b>CHCO</b>	Chief Human Capital Office or Officer
<b>CHWG</b>	Cyber Hygiene Working Group
<b>CIO</b>	Chief Information Officer
<b>CISA</b>	Cybersecurity and Information Sharing Act of 2015
<b>CMA</b>	Computer Matching Agreement
<b>COR</b>	Contracting Officer Representative
<b>CRCL</b>	Office for Civil Rights and Civil Liberties
<b>CS&amp;C</b>	Office of Cybersecurity & Communications in NPPD
<b>CUI</b>	Controlled Unclassified Information
<b>CVE</b>	Countering Violent Extremism
<b>CVTF</b>	Common Vetting Task Force
<b>DARC</b>	Data Access Review Council
<b>DHS</b>	Department of Homeland Security
<b>DHS TRIP</b>	DHS Traveler Redress Inquiry Program
<b>DMAG</b>	Deputy Secretary's Management Action Group
<b>DOJ</b>	Department of Justice
<b>DPIAC</b>	Data Privacy and Integrity Advisory Committee
<b>DPPA</b>	Data Protection and Privacy Agreement
<b>E3A</b>	EINSTEIN 3 Accelerated Program
<b>ECS</b>	Enhanced Cybersecurity Services
<b>EO</b>	Executive Order
<b>ESTA</b>	Electronic System for Travel Authorization
<b>EU</b>	European Union
<b>FACA</b>	Federal Advisory Committee Act
<b>FBI</b>	Federal Bureau of Investigation
<b>FCC</b>	Five Country Conference

<b>Acronym List</b>	
<b>FEMA</b>	Federal Emergency Management Agency
<b>FIPPs</b>	Fair Information Practice Principles
<b>FISMA</b>	Federal Information Security Management Act of 2002
<b>FLETC</b>	Federal Law Enforcement Training Centers
<b>FOIA</b>	Freedom of Information Act
<b>FPS</b>	Federal Protective Service
<b>FY</b>	Fiscal Year
<b>GSA</b>	General Services Administration
<b>HDI-WG</b>	Human Directive Intelligence Working Group
<b>HR</b>	Human Resources
<b>HSIN</b>	Homeland Security Information Network
<b>HQ</b>	Headquarters
<b>HSI</b>	Homeland Security Investigations
<b>I&amp;A</b>	Office of Intelligence and Analysis
<b>IAPP</b>	International Association of Privacy Professionals
<b>IC</b>	Intelligence Community
<b>ICAM</b>	Identity, Credentialing, and Access Management
<b>ICDPPC</b>	International Conference Data Protection & Privacy Commissioners
<b>ICE</b>	United States Immigration and Customs Enforcement
<b>IdM</b>	Identity Management
<b>IGA</b>	Office of Intergovernmental Affairs
<b>IGB</b>	International Governance Board
<b>IIR</b>	Intelligence Information Report
<b>IOC</b>	Initial Operational Capability
<b>IRS</b>	Internal Revenue Service
<b>ISA-IPC</b>	Information Sharing and Access Interagency Policy Committee
<b>ISAA</b>	Information Sharing Access Agreement
<b>ISAC</b>	Information Sharing and Analysis Center
<b>ISAO</b>	Information Sharing Analysis Organization
<b>ISCC</b>	Information Sharing Coordinating Council
<b>ISE</b>	Information Sharing Environment
<b>ISIL</b>	Islamic State of Iraq and the Levant
<b>ISP</b>	Internet Service Provider
<b>ISSGB</b>	Information Sharing and Safeguarding Governance Board
<b>ISSM</b>	Information Security System Manager
<b>ISSO</b>	Information Security System Officer
<b>IT</b>	Information Technology
<b>ITAR</b>	Information Technology Acquisition Review
<b>ITF</b>	Integrated Task Force
<b>ITP</b>	Insider Threat Program
<b>JRC</b>	Joint Requirements Council

<b>Acronym List</b>	
<b>LESMC</b>	Law Enforcement Shared Mission Community
<b>LPR</b>	License Plate Reader
<b>MMC</b>	Media Monitoring Capability
<b>NARA</b>	National Archives and Records Administration
<b>NCCIC</b>	National Cybersecurity and Communications Integration Center
<b>NCR</b>	National Capital Region
<b>NCTC</b>	National Counterterrorism Center
<b>NFIP</b>	National Flood Insurance Program
<b>NIST</b>	National Institute for Standards and Technology
<b>NOC</b>	National Operations Center
<b>NPPD</b>	National Protection and Programs Directorate
<b>NPRM</b>	Notice of Proposed Rulemaking
<b>NSTC</b>	National Science and Technology Council
<b>OBIM</b>	Office of Biometric Identity Management
<b>OCSO</b>	Office of the Chief Security Officer
<b>ODNI</b>	Office of the Director of National Intelligence
<b>OGC</b>	Office of the General Counsel
<b>OGIS</b>	Office of Government Information Services
<b>OIA</b>	TSA's Office of Intelligence and Analysis
<b>OIG</b>	Office of Inspector General
<b>OIP</b>	DOJ Office of Information Policy
<b>OMB</b>	Office of Management and Budget
<b>OPS</b>	Office of Operations Coordination
<b>OPM</b>	Office of Personnel Management
<b>PACT</b>	Privacy Administrative Coordination Team
<b>P/CL</b>	Privacy and civil liberties
<b>PCLOB</b>	Privacy and Civil Liberties Oversight Board
<b>PCR</b>	Privacy Compliance Review
<b>PIA</b>	Privacy Impact Assessment
<b>PII</b>	Personally Identifiable Information
<b>PIHG</b>	DHS Privacy Incident Handling Guidance
<b>PIV</b>	Personal Identity Verification
<b>PLCY</b>	Office of Policy
<b>PNR</b>	Passenger Name Records
<b>PPD</b>	Presidential Policy Directive
<b>PPOC</b>	Privacy Point of Contact
<b>PRA</b>	Paperwork Reduction Act
<b>PTA</b>	Privacy Threshold Analysis
<b>RO</b>	Reports Officer
<b>S&amp;T</b>	Science and Technology Directorate
<b>SAC</b>	Staff Advisory Council

---

### Acronym List

<b>SAOP</b>	Senior Agency Officials for Privacy
<b>SBA</b>	United States Small Business Administration
<b>SBU</b>	Sensitive but Unclassified
<b>SCO</b>	Screening Coordination Office
<b>SLTT</b>	State, Local and Tribal Territories
<b>SME</b>	Subject Matter Expert
<b>SMOUT</b>	Social Media Operational Use Template
<b>SOC</b>	Security Operations Center
<b>SORN</b>	System of Records Notice
<b>SOP</b>	Standard operating procedure
<b>SOW</b>	Statement of Work
<b>SSI</b>	Sensitive Security Information
<b>TSA</b>	Transportation Security Administration
<b>UAS</b>	Unmanned Aircraft Systems
<b>US-CERT</b>	United States Computer Emergency Readiness Team
<b>USCG</b>	United States Coast Guard
<b>USCIS</b>	United States Citizenship and Immigration Services
<b>USSS</b>	United States Secret Service

---

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

DHS's implementation of the FIPPs is described below:

**Transparency:** DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII. Technologies or systems using PII must be described in a SORN and PIA, as appropriate. There should be no system the existence of which is a secret.

**Individual Participation:** DHS should involve the individual in the process of using PII. DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

**Purpose Specification:** DHS should specifically articulate the authority which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

**Data Minimization:** DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). PII should be disposed of in accordance with DHS records disposition schedules as approved by the National Archives and Records Administration.

**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.

---

## 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;<sup>50</sup>
- (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.

---

<sup>50</sup> 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 [https://www.whitehouse.gov/sites/default/files/omb/assets/a11\\_current\\_year/a11\\_2016.pdf](https://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a11_2016.pdf)

---

## PIAs

The E-Government Act of 2002 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.<sup>51</sup>

---

<sup>51</sup> 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](http://www.whitehouse.gov/omb/circulars_a130_a130trans4). It should be noted that OMB Circular No. A-130 was revised on July, 28, 2016, and can be found here: <https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf>. However, the prior version of Appendix I of A-130 is still current guidance until OMB issues new guidance for reporting and publication under the Privacy Act of 1974. This OMB guidance is being revised and will be issued as OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, to be released this calendar year. More information can be found here: <https://www.whitehouse.gov/blog/2016/07/26/managing-federal-information-strategic-resource/>

---

## 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.<sup>52</sup> 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.<sup>53</sup>

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.<sup>54</sup>

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.

---

<sup>52</sup> 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).

<sup>53</sup> 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).

<sup>54</sup> 5 U.S.C. § 552a(o).

## Appendix D – Published PIAs and SORNs

Privacy Impact Assessments Published July 1, 2015 – June 30, 2016		
Component	Name of System	Date Published
CBP	DHS/CBP/PIA-003(b) Automated Commercial Environment	7/30/2015
CBP	DHS/CBP/PIA-027 Southwest Border Pedestrian Exit Field Test	12/4/2015
CBP	DHS/CBP/PIA-025(a) 1-to-1 Facial Comparison Project	1/14/2016
CBP	DHS/CBP/PIA-007(e) Electronic System for Travel Authorization (ESTA)	2/24/2016
CBP	DHS/CBP/PIA-028 Regulatory Management Information System (RAMIS)	4/6/2016
CBP	DHS/CBP/PIA-029 Remedy Enterprise Services Management System	4/29/2016
CBP	DHS/CBP/PIA-030 Air Exit Field Trial - Departure Information Systems Test	6/14/2016
CBP	DHS/CBP/PIA-007(f) Electronic System for Travel Authorization (ESTA)	6/20/2016
DHS-wide	DHS/ALL/PIA-053 Financial Management Systems	7/29/2015
DHS-wide	DHS/ALL/PIA-054 Identity Intelligence Biometrics (I2B) Pilot	10/14/2015
DHS-wide	DHS/ALL/PIA-014(c) Personal Identity Verification (PIV) Identity Management System (IDMS) Update	10/21/2015
DHS-wide	DHS/ALL/PIA-038(b) Integrated Security Management System (ISMS) Update	11/25/2015
DHS-wide	DHS/ALL/PIA-052 DHS Insider Threat Program	7/13/2015
DHS-wide	DHS/ALL/PIA-047(a) Workman's Compensation Program - Medical Case Management Services (WC-MCMS) System Update	2/11/2016
DHS-wide	DHS/ALL/PIA-046(c) DHS Data Framework	3/31/2016
DHS-wide	DHS/ALL-027(e) Watchlist Service - FDNS	5/19/2016
DHS-wide	DHS/OIG/PIA-001(b) Enterprise Data System	7/10/2015
FEMA	DHS/FEMA/PIA-041 Operational Use of Social Media for Situational Awareness Initiative	4/22/2016
ICE	DHS/ICE/PIA-043 SharePoint Matter Tracking Systems	7/10/2015
ICE	DHS/ICE/PIA-015(g) Enforcement Integrated Database (EID) Law Enforcement Notification System (LENS) Update	9/22/2015
ICE	DHS/ICE/PIA-044 LeadTrac	11/3/2015

Privacy Impact Assessments Published July 1, 2015 – June 30, 2016		
Component	Name of System	Date Published
ICE	DHS/ICE/PIA-015(g) Enforcement Integrated Database (EID) Criminal History Information Sharing (CHIS) Program	1/20/2016
ICE	DHS/ICE/PIA-045 ICE Investigative Case Management (ICM)	6/17/2016
NPPD	DHS/NPPD/PIA-023 Infrastructure Protection (IP) Gateway	7/28/2015
NPPD	DHS/NPPD/PIA-029 Automated Indicator Sharing	11/3/2015
NPPD	DHS/NPPD/PIA-028(a) Enhanced Cybersecurity Services (ECS)	12/1/2015
NPPD	DHS/NPPD/PIA-018(b) Chemical Facility Anti-Terrorism Standards (CFATS) Personnel Surety Program Update	12/18/2015
NPPD	DHS/NPPD/PIA-029(a) Automated Indicator Sharing (AIS)	3/15/2016
NPPD	DHS/PIA/NPPD-027(a) EINSTEIN 3 - Accelerated (E3A)	5/9/2016
OPS	DHS/OPS/PIA-009(a) National Operations Center Identity Targeting and Analysis Section (ITAS) Database	8/28/2015
S&T	DHS/S&T/PIA-028(a) Air Entry/Exit Re-engineering (AEER) Counting and Measuring Update	11/30/2015
TSA	DHS/TSA/PIA-029 - Operations Center Information Management System (OCIMS)	8/26/2015
TSA	DHS/TSA/PIA-006(a) Crew Vetting Program Update	10/20/2015
TSA	DHS/TSA/PIA-032(d) TSA Advanced Imaging Technology (AIT)	12/21/2015
TSA	DHS/TSA/PIA-041(b) Pre-check Application Program Update	2/10/2016
USCG	DHS/USCG/PIA-021 Rescue 21	7/29/2015
USCG	DHS/USCG/PIA-023 Incident Reporting Information System (IRIS)	9/18/2015
USCG	DHS/USCG/PIA-019(a) Transportation Worker Identification Credential (TWIC) Reader Requirements for U.S. Coast Guard	10/14/2015
USCG	DHS/USCG/PIA-022 Coast Guard Maritime Information eXchange (CGMIX)	7/30/2015
USCIS	DHS/USCIS/PIA-052 Electronic Workload Reporting and Tracking System (EWRTS)	7/10/2015
USCIS	DHS/USCIS/PIA-057 National Appointment Scheduling System (NASS)	7/30/2015

Privacy Impact Assessments Published July 1, 2015 – June 30, 2016		
Component	Name of System	Date Published
USCIS	DHS/USCIS/PIA-058 System Electronic Registration Approval (SERA)	9/29/2015
USCIS	DHS/USCIS/PIA-059 Known Employer Document Library (KEDL)	9/29/2015
USCIS	DHS/USCIS/PIA-056 Electronic Immigration System (ELIS)	11/3/2015
USCIS	DHS/USCIS/PIA-060 Customer Profile Management System (CPMS)	12/21/2015
USCIS	DHS/USCIS/PIA-030(f) E-Verify Mobile Application	1/20/2016
USCIS	DHS/USCIS/PIA-010 Person Centric Query Service (PCQS)	3/10/2016
USCIS	DHS/USCIS/PIA-062 Administrative Appeals Office (AAO) Case Management System	4/29/2016
USCIS	DHS/USCIS/PIA-013(a) Fraud Detection and National Security Data System (FDNS-DS)	5/23/2016
USCIS	DHS/USCIS/PIA-048(a) International Biometric Processing Services	5/31/2016
USCIS	DHS/USCIS/PIA-061 Benefit Request Intake Process	6/24/2016
USCIS	DHS/USCIS/PIA-016(a) Computer Linked Application Information Management System 3 (CLAIMS 3)	6/24/2016
USCIS	DHS/USCIS/PIA-063 Benefit Decision and Output	6/24/2016
USSS	DHS/USSS/PIA-015 eAgent	7/15/2015
USSS	DHS/USSS/PIA-012(a) Electronic Name Check System (E-Check)	7/30/2015

System of Records Notices Published July 1, 2015 – June 30, 2016		
Component	Name of System	Date Published
CBP	DHS/CBP-001 Import Information System (IIS)	8/17/2015
CBP	DHS/CBP-007 Border Crossing Information (BCI)	1/25/2016
CBP	DHS/CBP-009 Electronic System for Travel Authorization (ESTA)	2/23/2016
CBP	DHS/CBP-009 Electronic System for Travel Authorization (ESTA)	6/17/2016
CBP	DHS/CBP-014 Regulatory Audit Archive System	4/6/2016
CBP	DHS/CBP-020 Export Information System (EIS)	9/2/2015
CBP	DHS/CBP-021 Arrival Departure Information System (ADIS)	11/18/2015
DHS-wide	DHS/ALL-007 Accounts Payable Records	9/28/2015
DHS-wide	DHS/ALL-008 Accounts Receivable Records	9/28/2015
DHS-wide	DHS/ALL-010 Asset Management Records	9/28/2015
DHS-wide	DHS/ALL-019 Payroll, Personnel, Time, and Attendance Records System	9/28/2015
DHS-wide	DHS/ALL-030 Use of Terrorist Screening Database System	1/22/2016
DHS-wide	DHS/ALL-030 Use of Terrorist Screening Database System	4/6/2016
DHS-wide	DHS/ALL-038 Insider Threat Program	2/26/2016
OIG	DHS/OIG-002 Investigative Records System	7/27/2015
FEMA	DHS/FEMA-013 Operational Use of Social Media for Situational Awareness	4/21/2016
USCG	DHS/USCG-029 Notice of Arrival and Departure	11/30/2015
USCIS	DHS/USCIS-010 Asylum Information and Pre-Screening	11/30/2015

---

## 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:

### *September 2015*

- Data Privacy and Integrity Advisory Committee Meeting, Washington, DC
- Privacy Law Salon, George Washington Law School, Washington, DC

### *October 2015*

- Amsterdam Privacy Conference, The Netherlands

### *November 2015*

- Government Technology Research Alliance Conference, Hot Springs, Virginia
- Meritalk's Big Data Brainstorm, Washington, DC

### *December 2015*

- Federal Privacy Summit sponsored by the Federal CIO Council Privacy Committee, Washington, DC
- FedScoop's 2015 EDGE Summit, Washington, DC
- International Association of Privacy Professionals' Practical Privacy Series, Washington, DC

### *January 2016*

- International Association of Privacy Professionals Cyber Symposium, Jacksonville, FL

### *February 2016*

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

### *March 2016*

- Biometrics Institute Member Meeting, Washington, DC

### *April 2016*

- International Association of Privacy Professionals Global Privacy Summit, Washington, DC
- RSA Conference, San Francisco, California

### *May 2016*

- American Bar Association's Public Contract Law Section Roundtable, Washington, DC

### *June 2016*

- Business Forward Member Meeting, Washington, DC

---

## **Appendix F – Congressional Testimony and Staff Briefings**

### **Congressional Testimony**

The Chief Privacy Officer did not testify at any congressional hearings during the reporting period.

Historical written testimony can be found on the Privacy Office website: [www.dhs.gov/privacy](http://www.dhs.gov/privacy).

### **Congressional Staff Briefings**

Privacy Office staff, including the Chief Privacy Officer, briefed Congress several times during the reporting period on a range of issues, including: DHS privacy policy, Privacy Office activities, and the Social Media Task Force.

---

## 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:

<b>COUNTRY</b>	<b>ORGANIZATION/OFFICIAL</b>
Canada	Privy Council
Canada	Privacy Commissioner
Canada	Public Safety Canada
Canada	Immigration, Refugees & Citizenship
Canada	Business Council
Colombia	Communications & Appropriations, e-Government Division
Germany	National Business Daily
Hungary	National Authority of Data Protection & Freedom of Information
Norway	Ministry of Justice & Public Security
Poland	Ministry of Administration & Digitization
Romania	APADOR-CH (The Romanian Helsinki Committee)
Slovak Republic	Computer Security Incidence Response Team