Department of Homeland Security

Privacy Office

Fiscal Year 2016 Semiannual Report to Congress

For the period October 1, 2015 – March 31, 2016

July 6, 2016

Homeland Security

FOREWORD

July 6, 2016

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's *Fiscal Year 2016 Semiannual Report to Congress*, covering the time period October 1, 2015 – March 31, 2016.[1]

Highlights

During the reporting period, the Privacy Office:

- Issued a new privacy policy setting minimum privacy requirements for DHS mobile applications and developed a process so these requirements are implemented during mobile application development.
- Published government-wide best practices guidance, in collaboration with the Department's Unmanned Aircraft Systems Privacy, Civil Rights, and Civil Liberties Working Group, to assist government agencies in building unmanned aircraft system programs founded on strong privacy, civil rights, and civil liberties protections.
- Received advice from the Privacy Office's Federal Advisory Committee, the Data Privacy and Integrity Advisory Committee, in response to DHS Privacy's request for methods to protect privacy while achieving the cybersecurity goals of behavioral analysis throughout the information lifecycle.
- Issued two major reports to Congress:
  - *2015 Annual Report to Congress*
  - *2015 Data Mining Report to Congress*

About the Privacy Office

The *Homeland Security Act of 2002* 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 Chief Privacy Officer serves as the principal advisor to the DHS Secretary on privacy policy.

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. The Privacy Office undertakes these statutory and policy-based responsibilities in collaboration with DHS Component privacy[2] and FOIA officers, privacy points of contact (PPOC), and program offices to ensure that all privacy and disclosure issues are afforded the appropriate level of review and expertise.

[1] 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. 42 U.S.C. § 2000ee-1 (2014), Pub. L. No. 113-126, Title III, § 329(b)(4), 128 Stat. 1406 (2014). The DHS Privacy Office semiannual reports will cover the following time periods: April – September and October – March.

[2] Most DHS Components have a Privacy Officer or Privacy Point of Contact. Contact information can be found here: http://www.dhs.gov/privacy-office-contacts.

Please direct any inquiries about this report to the Privacy Office at 202-343-1717 or privacy@dhs.gov, or consult our website: www.dhs.gov/privacy.

Sincerely,

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

Pursuant to congressional notification requirements, the Privacy Office provides this report 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

Privacy Office
Fiscal Year 2016
Semiannual
Section 803 Report to Congress

Table of Contents

LEGISLATIVE LANGUAGE

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*,[3] as amended, sets forth the following requirements:

"(f) Periodic Reports-

(1) In General –

The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than semiannually, submit a report on the activities of such officers—

(A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;

(ii) to the head of such department, agency, or element; and

(iii) to the Privacy and Civil Liberties Oversight Board; and

(B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) Contents –

Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—

(A) information on the number and types of reviews undertaken;

(B) the type of advice provided and the response given to such advice;

(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and

(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer."

[3] 42 U.S.C. § 2000ee-1(f).

I. PRIVACY REVIEWS

The Privacy Office reviews programs and information technology (IT) systems that may have a privacy impact. For purposes of this report, reviews include the following:

1. Privacy Threshold Analyses, which are the DHS foundational mechanism for reviewing IT systems, programs, and other activities for privacy protection issues to determine whether a more comprehensive analysis is necessary, either through, e.g., by completing a Privacy Impact Assessment or a Systems of Records Notice;
2. Privacy Impact Assessments, as required under the *E-Government Act of 2002*,[4] the *Homeland Security Act of 2002*,[5] and DHS policy;
3. System of Records Notices, as required under the Privacy Act, and any associated Final Rules for Privacy Act exemptions;[6]
4. Privacy Act Statements, as required under the Privacy Act,[7] to provide notice to individuals at the point of collection;
5. Computer Matching Agreements, as required under the Privacy Act;[8]
6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*;[9]
7. Privacy Compliance Reviews, per the authority granted to the Chief Privacy Officer by the *Homeland Security Act of 2002*;[10]
8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) Exhibit 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board;
9. Information Technology Acquisition Reviews[11] (ITAR); and
1. Other privacy reviews, such as implementation reviews for public-facing information sharing agreements.

---

[4] 44 U.S.C. § 3501 note. *See also* OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), *available at*: http://www.whitehouse.gov/omb/memoranda_m03-22.

[5] 6 U.S.C. § 142.

[6] 5 U.S.C. § 552a(j), (k). 5 U.S.C. § 552a(e)(4). *See also* OMB Circular No. A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6428 (Feb. 20, 1996), *as amended*, 65 Fed. Reg. 77,677 (Dec. 12, 2000), *available at*: https://www.whitehouse.gov/omb/circulars_a130.

[7] 5 U.S.C. § 552a(e)(3).

[8] 5 U.S.C. § 552a(o)-(u).

[9] 42 U.S.C. § 2000ee-3.

[10] The Chief Privacy Officer and DHS Privacy Office exercises its authority under Section 222 of the Homeland Security Act (6 U.S.C. § 142) to assure that technologies sustain and do not erode privacy protections through the conduct of PCRs. Consistent with the Privacy Office's unique position as both and advisor and oversight body for the Department's privacy sensitive programs and systems, the PCR is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation.

[11] Section 208 of the E-Government Act requires that agencies conduct a privacy impact assessment (PIA) before procuring information technology (IT) that collects, maintains, or disseminates information that is in an identifiable form. DHS meets this requirement, in part, by participating in the Information Technology Acquisition Review (ITAR) process. The DHS Privacy Office reviews these ITAR requests to determine if the IT acquisitions require a new PIA to identify and mitigate privacy risks or if they are covered by an existing DHS PIA. In addition, the DHS Privacy Office reviews ITAR requests to ensure that appropriate language to safeguard personally identifiable information (PII) and Sensitive PII is included in new and existing contracts and solicitations that have a high risk of unauthorized access to, or disclosure of, sensitive information.

Table I **Privacy Reviews Completed:** ***October 1, 2015 – March 31, 2016***	
Type of Review	***Number of Reviews***
Privacy Threshold Analyses	297
Privacy Impact Assessments	25
System of Records Notices and associated Privacy Act Exemptions	11
Privacy Act (e)(3) Statements	7
Computer Matching Agreements	7
Data Mining Reports	1
Privacy Compliance Reviews	0
Privacy Reviews of IT and Program Budget Requests[12]	0
Information Technology Acquisition Reviews[13] (ITAR)	178
Other Privacy Reviews	0
Total Reviews	***526***

[12] The Chief Information Office prepares a privacy score once a year as part of its Office of Management and Budget Exhibit 300 reporting. Reviews for this category are calculated only during the second semi-annual reporting period.
[13] The DHS Privacy Office initiated ITAR reviews in January 2016.

Privacy Impact Assessments

The Privacy Impact Assessment (PIA) process is one of the Department's key mechanisms to ensure that DHS programs and technologies sustain, and do not erode, privacy protections. In addition to completing PIAs for new systems and projects, programs, pilots, or information sharing arrangements not currently subject to a PIA, the Department also conducts a triennial review of existing PIAs to assess and confirm that the systems still operate within the original parameters. After the triennial review, the Department updates any previously published PIAs, when needed, to inform the public that it has completed a review of the affected systems.

As of March 31, 2016, 88 percent of the Department's FISMA systems that require a PIA had an applicable PIA. During the reporting period, the Office published 25 PIAs: eight new and 17 updated. Included here are a summary of significant PIAs, along with a hyperlink to the full text.

All published DHS PIAs are available on the Privacy Office website, www.dhs.gov/privacy.

DHS/NPPD/PIA-029 Automated Indicator Sharing (AIS) *(October 28, 2015, updated and republished March 16, 2016).*
The DHS National Protection and Programs Directorate's (NPPD) Office of Cybersecurity and Communications (CS&C) developed an Automated Indicator Sharing (AIS) initiative to enable 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 the Cybersecurity Information Sharing Act of 2015 (CISA) in a manner that ensures appropriate incorporation of privacy, civil liberties, and other compliance protections. Central to the AIS initiative and consistent with the requirements of CISA, the DHS National Cybersecurity and Communications Integration Center (NCCIC) serves as the centralized hub for exchanging cybersecurity threat information using a DHS-accredited infrastructure. NPPD conducted this PIA because personally identifiable information (PII) may be submitted as part of or accompanying a cyber threat indicator or defensive measure.

DHS/USCIS/PIA-056 USCIS Electronic Immigration System (USCIS ELIS) *(October 30, 2015).*
The United Stated Citizenship and Immigration Service (USCIS) operates the USCIS Electronic Immigration System (USCIS ELIS). USCIS ELIS is an electronic case management system that allows USCIS to process certain immigration benefit requests. USCIS conducted this PIA to evaluate the privacy impacts of converting legacy, paper-based processes to an electronic system. This PIA replaces all previously-issued USCIS ELIS PIAs, which are: DHS/USCIS/PIA-039 Transformation, DHS/USCIS/PIA-041 ELIS-1 Temporary Accounts and Draft Benefit Requests, DHS/USCIS/PIA-042 ELIS-2 Account and Case Management, DHS/USCIS/PIA-043 ELIS-3 Automated Background Functions, and DHS/USCIS/PIA-056 USCIS ELIS: Form I-90. As USCIS ELIS expands to additional immigration benefit types, USCIS will update the Appendix to this PIA.

DHS/CBP/PIA-027 Southwest Border Pedestrian Exit Field Test *(November 6, 2015).*
U.S. Customs and Border Protection (CBP) is conducting 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 is 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 collects PII about members of the public.

DHS/NPPD/PIA-028(a) Enhanced Cybersecurity Services (ECS) (*updated November 30, 2015).*
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. NPPD conducted this PIA Update to reflect ECS' support by Executive Order 13636, Improving Critical Infrastructure Cybersecurity, announce the expansion of service beyond Critical Infrastructure sectors to all U.S.-based public and private entities, and to introduce the new Netflow Analysis service.

DHS/TSA/PIA-032(d) Advanced Imaging Technology *(updated December 18, 2015).*
The Transportation Security Administration (TSA) has 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 (ATR) software to display the location of the object on a generic figure as opposed to displaying the image of the individual. TSA updated the AIT PIA to reflect a change to the operating protocol regarding the ability of individuals to opt 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. TSA does not store any PII from AIT screening.

DHS/TSA/PIA-041(a) TSA Pre✓™ Application Program *(updated January 22, 2016).*
TSA operates its TSA Pre✓® Application Program to perform a security threat assessment on individuals who seek eligibility for expedited screening at participating U.S. airport security checkpoints. This PIA update covers two aspects of the program: 1) TSA's offer to obtain a birth certificate certification through the National Association for Public Health Statistics and Information Systems (NAPHSIS); and 2) TSA expansion of TSA Pre✓® Application Program capabilities by entering into agreements with private-sector entities for marketing, enrollment, identity assurance, and criminal records checks. As part of the latter expansion effort, TSA will share PII collected by the TSA Pre✓® Application Program with DHS Science & Technology (S&T) Directorate to test the ability of the private sector to perform identity assurance and criminal history assessments.

DHS/ALL/PIA-052 DHS Insider Threat Program *(January 5, 2016).*
The DHS Insider Threat Program (ITP) is a department-wide effort established pursuant to Executive Order No. 13587 "Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information," to protect classified national security information from unauthorized disclosure. 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 Information Technology (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.

DHS/CBP/PIA-025 1:1 Facial Comparison Project *(January 14, 2016).*
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 (CBPO) 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 CBPOs in making admissibility determinations.

DHS/CBP/PIA-028 Regulatory Management Information System *(March 14, 2016).*
CBP uses the Regulatory Management Information System (RAMIS) to conduct post-entry regulatory audits of importers, brokers, and other parties involved in international trade activities. Its associated repository, the Regulatory Audit Archive System (RAAS), stores completed audit documentation and reports compiled by RAMIS. These audits enable revenue collection, facilitate legitimate trade, provide a compliance framework to the trade community, and deter future trade violations. CBP conducted this PIA because this system collects PII about members of the public.

DHS/ALL/PIA-046(c) DHS Data Framework *(updated March 30, 2016).*
The DHS Data Framework is DHS's "big data" solution to build in privacy protections while enabling more controlled, effective, and efficient use of existing homeland security-related information. The DHS Data Framework includes the Neptune and Cerberus systems. DHS updated the Data Framework PIA to reflect that DHS will now use Cerberus to share information externally, including "bulk information sharing," with U.S. Government partners, consistent with information sharing access agreements, published PIAs and System of Records Notices (SORN) for the underlying source systems of the DHS Data Framework.

DHS/ICE/PIA-044 LeadTrac System (*October 30, 2015*).
LeadTrac is a database owned by the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Counterterrorism and Criminal Exploitation Unit (CTCEU). The function of LeadTrac is to vet and manage leads pertaining to visitors in 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. CTCEU and the Overstay Analysis Unit conduct research and enrich the leads in LeadTrac, and, when appropriate, refer them to ICE field offices for investigation and enforcement action.

DHS/ICE/PIA-015(h) Enforcement Integrated Database (EID) Criminal History Information Sharing (CHIS) Program (*updated January 15, 2016*).
Since 2010, ICE has shared certain criminal history information with foreign countries concerning nationals of those countries who are being repatriated from the United States and who were convicted of certain felonies in the United States. This information sharing effort is referred to as the CHIS program, and is formalized by cooperation agreements between DHS and each participating country. ICE shares the information provided through the CHIS program from the EID, which is a DHS shared common database repository for several DHS law enforcement and homeland security applications. EID captures and maintains information related to the investigation, arrest, booking, detention, and removal of persons encountered during immigration and criminal law enforcement investigations and operations conducted by ICE and CBP. This update to the EID PIA describes a change to the CHIS

program whereby ICE will use a secure web service to share this criminal history information with its foreign partners.

System of Records Notices

The Department publishes System of Records Notices (SORN) consistent with the requirements outlined in the *Privacy Act of 1974*.[14] The Department conducts biennial reviews of SORNs to ensure that they conform to and comply with the standards outlined in the Privacy Act. If no update is required, the original SORN remains in effect.

As of March 31, 2016, 98 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the Office published seven SORNs: one new and six updated. Included here are a summary of significant SORNs, along with a hyperlink to the full text in the *Federal Register*.

All DHS SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act Exemptions are available on the Privacy Office website, www.dhs.gov/privacy.

DHS/CBP-021 Arrival Departure Information System (ADIS) (update)
This system of records authorizes CBP to collect and maintain records on individuals throughout the immigrant and non-immigrant pre-entry, entry, status management, and exit processes. DHS/CBP updated this system of records notice to make the following changes/updates: (1) Addition of a new category of records; (2) updated routine uses; and (3) administrative updates to reflect the transfer of the entry-exit program from the Office of Biometric Identity Management, an office within DHS, National Protection and Programs Directorate, to CBP in accordance with the Consolidated and Further Continuing Appropriations Act of 2013. *(80 Fed. Reg. 72081, November 18, 2015)*

DHS/USCIS-010 Asylum Information and Pre-Screening (update)
This system of records authorizes USCIS to collect and maintain records pertaining to asylum applications, credible fear and reasonable fear screening processes, and applications for benefits provided by section 203 of the Nicaraguan Adjustment and Central American Relief Act. USCIS updated this SORN to: (1) clarify that data originating from this system of records may be stored in a classified network; (2) provide an updated system location; (3) include follow-to-join (derivative) asylum information as a category of records; (4) expand the categories of records for benefit requestors, beneficiaries, derivatives, accredited representatives (including attorneys), form preparers, and interpreters; (5) remove routine use K because it was duplicative; (6) add two new routine uses K and L to permit the sharing of information with the Departments of State and Health and Human Services, respectively; (7) update the retention schedules to include additional systems; (8) add name and date of birth combination and receipt number to retrieve records; and (9) update record source categories to include accredited representatives (including attorneys), interpreters, preparers, and USCIS personnel. *(80 Fed. Reg. 74781, November 30, 2015)*

[14] 5 U.S.C. § 552a(j), (k). 5 U.S.C. § 552a(e)(4). *See also* OMB Circular No. A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals, 61 Fed. Reg. 6428 (Feb. 20, 1996), *as amended*, 65 Fed. Reg. 77,677 (Dec. 12, 2000), *available at*: https://www.whitehouse.gov/omb/circulars_a130.

DHS/USCG-029 Notice of Arrival and Departure (update)
This system of records authorizes the United States Coast Guard (Coast Guard) to collect information regarding entry and departure of vessels into and from the United States, and assist with assigning priorities for complying with maritime safety and security regulations. The Coast Guard updated this SORN to update the (1) authority for maintenance of the system, (2) security classification, (3) system location, (4) purpose(s), (5) categories of individuals, (6) categories of records, (7) routine uses, (8) retention and disposal, (9) notification procedures, and (10) system manager and address. *(80 Fed. Reg. 74116, November 30, 2015)*

- DHS/USCG-029 Notice of Arrival and Departure, Notice of Proposed Rulemaking for Privacy Act Exemptions
  Concurrent with the NOAD SORN update, DHS updated the associated NOAD rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. *(80 Fed. Reg. 74018, November 27, 2015)*

DHS/ALL-030 Use of the Terrorist Screening Database System (update)
This system of records authorizes the DHS to maintain a synchronized copy of the Department of Justice's (DOJ) Federal Bureau of Investigation's (FBI) Terrorist Screening Database (TSDB), which includes categories of individuals covered by DOJ/FBI-019, "Terrorist Screening Records Center System," 72 FR 77846, Dec. 14, 2011. DHS maintains a synchronized copy to automate and simplify the transmission of information in the Terrorist Screening Database to DHS and its components. With this updated notice, DHS added two new consumers, CBP Automated Targeting System (ATS), and USCIS Fraud Detection and National Security (FDNS) Directorate, to the "DHS Watchlist Service." DHS also clarified an existing category of individuals, added two new categories of individuals, and clarified the categories of records maintained in this system. *(81 Fed. Reg. 19988, January 22, 2016, updated and reissued April 6, 2016)*

- DHS/ALL-030 Use of the Terrorist Screening Database System, Final Rule for Privacy Act Exemptions
  Concurrent with the reissuance of the TSDB SORN, DHS published a Final Rule in which the Department exempted portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. *(81 Fed. Reg. 19857, April 6, 2016)*

DHS/CBP-007 Border Crossing Information (update)
This system of records authorizes CBP to collect and maintain records on border crossing information for all individuals who enter, are admitted or paroled into, and (when available) exit from the United States, regardless of method or conveyance. Border Crossing Information (BCI) includes certain biographic and biometric information; photographs; certain mandatory or voluntary itinerary information provided by air, sea, bus, and rail carriers or any other forms of passenger transportation; and the time and location of the border crossing. CBP updated this SORN to provide notice that BCI may be stored on both DHS unclassified and classified networks to allow for analysis and vetting consistent with existing CBP authorities and purposes, and this published notice. Furthermore, this notice included non-substantive changes to simplify the formatting and text of the previously published notice. *(81 Fed. Reg. 404, January 25, 2016)*

- DHS/CBP-007 Border Crossing Information, Final Rule for Privacy Act Exemptions
  Concurrent with the reissuance of the BCI SORN, DHS issued a final rule to extend the exemptions from certain provisions of the Privacy Act to the updated and reissued system of records titled, "DHS/U.S. Customs and Border Protection (CBP)-007 Border Crossing Information System of Records." Specifically, the Department exempts portions of the "DHS/CBP-007 Border Crossing Information System of Records" from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. *(81 Fed. Reg. 14947, March 21, 2016)*

DHS/CBP-009 Electronic System for Travel Authorization (update)
This system of records authorizes CBP to collect and maintain records on nonimmigrant aliens seeking to travel to the United States under the Visa Waiver Program and other persons, including U.S. citizens and lawful permanent residents, whose names are provided to DHS as part of a nonimmigrant alien's Electronic System for Travel Authorization (ESTA) application. The system is used to determine whether an applicant is eligible to travel to and enter the United States under the Visa Waiver Program (VWP) by vetting his or her ESTA application information against selected security and law enforcement databases at DHS, including but not limited to TECS (not an acronym) and ATS.

CBP updated this system of records notice, last published on November 4, 2014 (79 FR 65414), to modify the categories of records in the system to include responses to new questions and additional data elements to assist CBP in determining eligibility to travel under the VWP. DHS also modified the categories of records to remove several data elements that are no longer collected, including date of anticipated crossing, carrier information (carrier name and flight or vessel number), city of embarkation, and any change of address while in the United States. In 2014, CBP determined that these fields were unnecessary for mission operations. CBP also revised the ESTA application to reflect the current quarantinable, communicable diseases specified by any Presidential E.O. under section 361(b) of the Public Health Service Act (PHS Act). Lastly, CBP made non-substantive, clarifying edits to Routine Use N. *(81 Fed. Reg. 8979, February 23, 2016)*

DHS/ALL-038 Insider Threat Program
This system authorizes DHS to manage insider threat inquiries, investigations, and other activities associated with complaints, inquiries, and investigations regarding the unauthorized disclosure of classified national security information; identification of potential threats to DHS resources and information assets; tracking of referrals of potential insider threats to internal and external partners; and providing statistical reports and meeting other insider threat reporting requirements. *(81 Fed. Reg. 9871, February 26, 2016)*

- DHS/ALL-038 Insider Threat Program System of Records, Notice of Proposed Rulemaking for Privacy Act Exemptions
  Concurrent with the Insider Threat SORN, DHS published a Notice of Proposed Rulemaking in which the Department proposed to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. *(81 Fed. Reg. 9789, February 26, 2016)*

Privacy Compliance Reviews

The Privacy Office uses Privacy Compliance Reviews (PCR) to ensure DHS programs and technologies implement and maintain appropriate privacy protections for Personally Identifiable Information (PII). Consistent with the Office's unique position as both an advisor and oversight body for the Department's privacy-sensitive programs and systems, the PCR is a collaborative effort that helps improve a program's ability to comply with existing privacy compliance documentation, including PIAs, SORNs, and formal agreements such as Memoranda of Understanding and Memoranda of Agreement. PCRs may result in public reports or internal recommendations, depending upon the sensitivity of the program under review.

The Office did not publish any PCRs during this reporting period.

All public PCRs are available on the Privacy Office website, www.dhs.gov/privacy, under Reviews and Investigations.

Data Mining Reports

In February 2016, the DHS Privacy Office published the *2015 Data Mining Report to Congress*. This report discusses activities currently deployed or under development at the Department that meet the *Data Mining Reporting Act's* definition of data mining, and provides the information set out in the Act's reporting requirements for data mining activities.

All Data Mining Reports are available on the Privacy Office website, www.dhs.gov/privacy, under Privacy & FOIA Reports.

II. ADVICE AND RESPONSES

The Privacy Office provides significant ongoing privacy policy leadership on a wide range of topics in various fora, as described in detail in the *2015 Privacy Office Annual Report to Congress*.

Highlights of significant accomplishments during this reporting period are summarized below.

Privacy Policy

The DHS Privacy Office published *Instruction 047-01-003, Privacy Policy for DHS Mobile Applications*. This Instruction implements *DHS Directive 047-01, Privacy Policy and Compliance*, concerning DHS mobile applications that are developed by, on behalf of, or in coordination with the Department, and are intended for use by DHS employees and/or the public. Most notably, this Instruction sets minimum privacy requirements for DHS mobile applications and ensures these requirements are implemented during the DHS mobile application development process.

Best Practices

The Department of Homeland Security's Unmanned Aircraft Systems Privacy, Civil Rights, and Civil Liberties Working Group published government-wide best practices guidance to assist government agencies in incorporating strong privacy, civil rights, and civil liberties protections as part of its unmanned aircraft system programs. These best practices are based on DHS Fair Information Practice Principles, and reflect the Department's considerable experience operating unmanned aircraft systems in securing the Nation's borders and supporting communities during natural disasters and emergencies.

While primarily intended for DHS and its local, state, and Federal Government partners and grantees, the private sector may also find these best practices valuable and instructive in creating unmanned aircraft system programs.

Information Sharing

The Privacy Office collaborates with Component privacy offices, the DHS Office of Intelligence and Analysis (I&A),[15] 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:

1. Provides leadership and privacy subject-matter expertise in DHS's ongoing evaluation of its information sharing with the Intelligence Community (IC).
    a. As part of DHS's DARC, the Office incorporates privacy best practices, such as protections related to transparency, oversight, and redress, into Information Sharing and Access Agreements (ISAA) with the IC.
    b. The Privacy Office continues to participate in quarterly reviews of the National Counterterrorism Center's (NCTC) use of DHS data, including its application of baseline safeguards.[16]

[15] 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.
[16] More information on NCTC's data stewardship is available through its Transparency Initiative at http://www.nctc.gov/transparency.html.

2. Advises on domestic and international information sharing agreements to ensure consistency with U.S. privacy law and DHS privacy policy, particularly on sharing that occurs through biometric-based query and response.
3. Maintains a leadership role in DHS's internal information sharing and management governance processes.

Publications

The Chief Privacy Officer tasked the Privacy Office's Federal Advisory Committee, the Data Privacy and Integrity Advisory Committee (DPIAC),[17] with providing recommendations to DHS to consider how best to address privacy protection in the conduct of "behavioral analytics" in cybersecurity programs.

In response, on February 17, 2016, the DPIAC issued *Report 2016-01, Recommendations on Algorithmic Analytics and Privacy Protection*. The report is structured in three sections, each of which contains insight and recommendations for DHS to consider:

1. general considerations regarding the scope of the DHS inquiry,
2. key considerations that impact algorithmic analytics, and
3. questions to address for major categories of information handling.

[17] The DPIAC provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to personally identifiable information, as well as data integrity and other privacy-related matters. The DPIAC was established by the Secretary of Homeland Security under the authority of 6 U.S.C. § 451 and operates in accordance with the provisions of the Federal Advisory Committee Act (FACA) (5 U.S.C. App). More information on the DPIAC can be found here: https://www.dhs.gov/privacy-advisory-committee.

III. Training and Outreach

Mandatory Online Training

90,529 DHS personnel completed the mandatory computer-assisted privacy awareness training course, *Privacy at DHS: Protecting Personal Information*. This course is required for all personnel when they join the Department, and annually thereafter.

15,887 DHS personnel completed Operational Use of Social Media Training during this reporting period, as required by *DHS Directive Instruction Number 110-01-001, Privacy Policy for Operational Use of Social Media*, and applicable Privacy Office-adjudicated Component Social Media Operational Use Template(s).

Classroom Training

5,638 DHS personnel attended instructor-led privacy training courses, including the following:

- New Employee Training: The Privacy Office provides privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees. Many of the Component Privacy Officers also offer privacy training for new employees in their respective Components. In addition, the Privacy Office provides 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 privacy staff in the Components in compliance best practices, including how to draft PTAs, PIAs and SORNs.
- FOIA Training: This periodic training is tailored to staff responsible for gathering records in response to FOIA requests, and for FOIA staff processing records.
- Nationwide Suspicious Activity Reporting Initiative: The Privacy Office provides training in privacy principles to Suspicious Activity Reporting analysts.
- DHS 201 International Attaché Training: The Department's "DHS 201" training module is a week-long course designed to prepare DHS employees who serve as DHS attachés at U.S. embassies worldwide by providing them with basic information on each Component's international activities. The Privacy Office provides an international privacy policy module to raise awareness among new attachés of the potential impact of global privacy policies.
- DHS 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 the Office for Civil Rights and Civil Liberties to provide periodic privacy training for privacy officers at state and local fusion centers.
- Privacy Briefings for Headquarters Staff: During this reporting period, the Privacy Office continued a year-long privacy awareness campaign throughout the DHS Headquarters division to provide customized classroom privacy awareness briefings to employees and contractors. The goal is to increase awareness of DHS privacy policy and the importance of incorporating privacy protections into any new program or system that will collect PII.

Outreach

- Biometrics Institute Meeting – On March 17, 2016, in Washington, DC, the Deputy Chief Privacy Officer participated in a panel discussion on how to promote strong privacy protections within government and industry.
- Privacy Advocate Meeting – On March 14, 2016, in Arlington, Virginia, privacy advocates met with the Chief Privacy Officer 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 (February 26, 2016).
- Data Privacy and Integrity Advisory Committee Meeting – On February 8, 2016, in Washington, DC, the Privacy Office hosted a public meeting of the Data Privacy and Integrity Advisory Committee (DPIAC). Members were briefed by Privacy Office senior management on 2016 priorities, and heard presentations from representatives of the Privacy and Civil Liberties Oversight Board and the new Federal Privacy Council. The committee discussed its research findings on algorithmic analytics and privacy protections, which can be found in *Report 2016-01 of the DHS Data Privacy and Integrity Advisory Committee on Algorithmic Analytics and Privacy Protection*.
- IAPP/FCBA Florida Privacy and Cyber Symposium – On January 28, 2016, in Jacksonville, Florida, the Chief Privacy Officer gave the keynote address on how the DHS approach to privacy can help inform private sector privacy program development.
- Fed Scoop's 2015 Edge Summit – On December 8, 2015, in Washington, DC, the Deputy Chief Privacy Officer participated in a panel presentation with the Chief Information Officer (CIO) of the Army to discuss best practices in balancing the needs of securing data while also protecting privacy.
- Federal Privacy Summit – On December 2, 2015, in Washington, DC, the CIO Council Privacy Committee, co-chaired by the Deputy Chief Privacy Officer, hosted a one-day workshop that convened budget, procurement, human resources, public affairs, congressional affairs, and intergovernmental affairs staff from DHS and other federal agencies to discuss privacy and security. Subject matter experts shared best practices for protecting privacy, and ways to improve collaboration across the enterprise. Shaun Donovan, Director, Office of Management and Budget, gave the keynote address.
- Meritalk's Big Data Brainstorm – On November 19, 2015, in Washington, DC, the Chief Privacy Officer gave the keynote address at the Newseum.
- Government Technology Research Alliance (GTRA) Conference – On November 15, 2015, in Hot Springs, Virginia, the Deputy Chief Privacy Officer participated on a panel discussion, *Privacy: Compliance, Objectives, Strategic Inclusion, and Key Concerns*.

Component Training and Outreach

Federal Emergency Management Agency (FEMA)

- Supported the agency's Workplace Transformation initiative by conducting privacy training and site risk analysis in the National Capital Region (NCR), and in targeted Regional Offices and field sites to reinforce best practices for securing PII during office relocations and disaster operations.
- Initiated expansion of the Privacy Office footprint into disaster operations offices and sites by having a PPOC on-site at each disaster to provide "just in time" privacy training, disseminate privacy resource materials, and conduct privacy compliance site assessments. The goal is to embed and improve privacy protection and oversight in FEMA disaster operations environments and reduce privacy incidents.
- Provided a privacy resource packet (consisting of privacy fact sheets, privacy posters, and best practice materials) to the Office of Response and Recovery, Individual Assistance Division, for inclusion in each Disaster Recovery Office set-up kit. The FEMA Privacy Office also disseminated these materials across the enterprise to enhance PII protection and privacy incident reporting and mitigation.
- Provided specialized privacy training to information management professionals, and remedial training as a result of privacy incidents or potential privacy risks.
- Served on the agency's Intranet Governance Working Group to establish governance on FEMA's use of SharePoint, specifically with respect to safeguarding PII.
- Requested staff complete mandatory annual online privacy training by April 1, 2016.

National Protection and Programs Directorate (NPPD)

- Partnered with the National Cybersecurity Communication Integration Center (NCCIC)/United States Computer Emergency Readiness Team (US-CERT) to provide cybersecurity information handling privacy training to employees in the Office of Cybersecurity and Communications.
- Presented to members of the Northern Virginia Technology Council's Cybersecurity and Privacy Committee on DHS's implementation of, and the privacy protections surrounding, the Automated Indicator Sharing (AIS) Initiative on November 18, 2015.
- Led a session on "Identity Management Across Functional Lines," at the 2015 CIO Council's Privacy Summit on December 3, 2015.
- Hosted the annual NPPD Privacy and Technology Workshop on December 7, 2015, an interactive technology fair presented by various NPPD program offices that featured topics such as security, privacy, malware, and encryption.
- Briefed the Federal Privacy Council, various privacy advocacy organizations, and several federal agencies on the CISA Privacy and Civil Liberties Interim Guidelines between December 2015 and March 2016.
- Participated in two panels, *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, on February 29, 2016.
- Provided a number of Privacy and Acquisitions trainings in February and March 2016, featuring the *Class Deviation 15-01 from the Homeland Security Acquisition Regulation: Safeguarding of Sensitive Information*, and the role of NPPD Privacy in the procurement process.
- Conducted Privacy Awareness 101 training to the Federal Protective Service Personnel Security Division on March 15, 2016.

- Participated in a panel discussion on *The Perception of Privacy on Biometrics* at a Biometrics Institute general membership meeting on March 17, 2016.
- Hosted a three-day Privacy Training Days Event, March 29-31, 2016, with sessions held at four directorate office locations, targeting employees and contractors in the NCR.
- Relaunched a quarterly newsletter in FY 2016, the *NPPD Privacy Update*, which is distributed NPPD-wide, and posted on the NPPD Office of Privacy Intranet page.

Office of the Chief Security Officer (OCSO)

- Provided a privacy training module in these OCSO classroom courses:
  - Security Orientation for Contractors
  - Security Orientation for Federal Employees
  - Safeguarding NSI: Your Responsibilities
  - Risk Management for Security Professionals
  - Operations Security
  - Sensitive But Unclassified Information
  - Acquisition Security Course
  - DHS Security Specialist Course. A DHS Privacy Office representative teaches the privacy module for this course.

Science and Technology Directorate (S&T)

- Presented at the American Conference Institute in January 2016 on *Emerging Threats and Evolving Remedies: Biometrics and Behavior Recognition.*

United States Citizenship and Immigration Services (USCIS)

- Briefed employees on two Office of Personnel Management data breaches.
- Updated the privacy intranet site and the regional privacy web pages with a new awareness resource page featuring links to privacy related policies, cybersecurity information, and Federal Trade Commission consumer privacy resources.
- Performed site visits and risk assessments of USCIS facilities, providing recommendations to leadership on ways to improve privacy protections and awareness.
- Provided a privacy compliance overview to the Forms Management Branch to ensure staff complete required privacy compliance documentation for all forms.
- Briefed the Customer Service and Public Engagement Directorate on how to prevent identity theft during tax season.
- Conducted a privacy briefing for all contractors supporting the Fraud Detection and National Security Directorate's Program Management Office and IT acquisition and development activities.
- Trained International Operations on USCIS privacy policies, focusing on Privacy Act principles and information sharing with third parties.
- Published an updated Regional and District Field Office Site Visit Template, with a more user-friendly format covering a broader range of privacy related topics.
- Published the USCIS Office of Privacy quarterly newsletter, *Privacy Chronicles*, to convey privacy incident reporting requirements and emphasize the importance of working together to ensure that privacy is incorporated into all USCIS policies, guidance, and procedures.
- Published agency-wide *Privacy Tips* to highlight the appropriate use, access, sharing and disposal of PII, and how to effectively report a privacy incident.

- Published a bi-annual thank you letter from the Chief Privacy Officer to USCIS leadership, thanking them for supporting a culture of privacy throughout the agency.
- Published a quarterly memo to all USCIS personnel to reinforce staff responsibility to safeguard PII.

U.S. Customs and Border Protection (CBP)

- Presented at four Office of Field Operations (OFO) audit refresher classes entitled *Roles and Responsibilities of OFO Personnel During the Audit Purpose*, training more than 215 OFO personnel on privacy.
- Collaborated with the Office of Information Technology to refresh the privacy section of the *2016 IT Computer Security Awareness and Rules of Behavior Training*.

U.S. Immigration and Customs Enforcement (ICE)

- ICE Privacy Officer gave the keynote address at the IAPP Practical Privacy Series on November 18, 2015.
- ICE Privacy Officer participated in a panel discussion on *How to Report a Privacy Incident* at the U.S. Department of Veterans Affairs on January 28, 2016.
- ICE Privacy Officer spoke on ICE Privacy's role in the acquisitions process to the ICE Acquisitions Community of Practice on March 17, 2016.

United States Secret Service (USSS)

- Trained 312 new Special Agents and Uniformed Division Officer recruits in privacy rules of behavior, including how to safeguard PII.
- Disseminated privacy awareness posters to Headquarters and Field Offices, and via the Intranet to encourage employees to properly handle and safeguard PII.
- Established a PII Working Group to assess the use, collection, maintenance and dissemination of PII within the Secret Service, and to identify additional privacy training needs to improve the handling and safeguarding of PII.
- Trained new hires on privacy protection best practices at bi-weekly new employee orientation classes.

IV. PRIVACY COMPLAINTS AND DISPOSITIONS

For purposes of Section 803 reporting, complaints are written allegations of harm or violations of privacy compliance requirements that are filed with the Privacy Office or DHS Components or programs. The categories of complaints reflected in the following table are aligned with the categories detailed in the Office of Management and Budget's Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 14, 2008)*. U.S. citizens, Lawful Permanent Residents, visitors, and aliens submit complaints.[18]

Table II: Type and Disposition of Complaints Received in the Reporting Period				
Type of Complaint	**Number of complaints received during the reporting period**	**Disposition of Complaint**		
		Closed, Responsive Action Taken[19]	**In Progress (Current Period)**	**In Progress (Prior Periods)**
Process & Procedure	9	10	2	3
Redress	254	255	0	0
Operational	777	807	34	3
Referred	12	9	0	0
Total	***1,052***	***1,081***	***36***	***6***

.

DHS separates complaints into four categories:

1. ***Process and Procedure****:* Issues concerning process and procedure, such as consent, or appropriate notice at the time of collection.
    a. *Example*: An individual submits a complaint that alleges a program violates privacy by collecting Social Security numbers without providing proper notice.
2. ***Redress***: Issues concerning appropriate access and/or correction of PII, and appropriate redress of such issues.
    a. *Example*: Misidentifications during a credentialing process or during traveler inspection at the border or screening at airports.[20]
3. ***Operational***: Issues related to general privacy concerns, and concerns not related to transparency or redress.
    a. *Example:* An employee's health information was disclosed to a non-supervisor.

[18] *See* DHS Privacy Policy Guidance Memorandum 2007-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons* (Jan. 7, 2009)., available here: http://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2007-01-regarding-collection-use-retention-and.

[19] These totals include complaints opened and closed during this reporting period, and complaints opened in prior reporting periods but closed during this reporting period.

[20] This category excludes FOIA and Privacy Act requests for access, which are reported annually in the Annual FOIA Report, and Privacy Act Amendment requests, which are reported annually in the DHS Privacy Office Annual Report to Congress.

4. ***Referred****:* The Privacy Office or another DHS Component determined that the complaint would be more appropriately handled by another federal agency or entity, and referred the complaint to the appropriate organization. This category does not include internal referrals within DHS. The referral category both serves as a category of complaints and represents responsive action taken by the Department, unless a complaint must first be resolved with the external entity.
    a. *Example*: An individual has a question about his or her driver's license or Social Security number, which the Privacy Office refers to the proper agency.

DHS Components and the Privacy Office report disposition of complaints in one of the two following categories:

1. *Closed, Responsive Action Taken*: The Privacy Office or another DHS Component reviewed the complaint and took responsive action. For example, an individual may provide additional information to distinguish himself from another individual. In some cases, acknowledgement of the complaint serves as the responsive action taken. This category may include responsive action taken on a complaint received from a prior reporting period.

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

The following are examples of complaints received during this reporting period, along with their disposition:

National Protection and Programs Directorate (NPPD)

COMPLAINT # 1: The NPPD Office of Privacy received a complaint from an NPPD employee who had concerns about their management's request to identify staff holding job-specific certifications. The manager wanted to post the individuals' names and certifications on an internal SharePoint site.

DISPOSITION: After the complaint was presented, the manager determined that posting such information to a SharePoint site was not necessary, and simply providing the data directly to leadership would be a better solution. The data was anonymized, and only the total number of personnel with job-related certifications was provided to leadership.

COMPLAINT # 2: The NPPD Office of Privacy received a complaint from an individual regarding the manner in which an NPPD contractor collected PII from federal employees. The contractor collected PII in order to issue identification badges to federal employees to provide them access to the contractor's offsite facility.

DISPOSITION: The Contracting Officer's Representative (COR) reviewed the contract and confirmed that this type of PII collection was intended only for very specific personnel access credentialing, and only on an as-needed basis. The process of collecting Sensitive PII for badge issuance for all federal staff was immediately halted, all relevant PII that had been collected by the contractor was deleted, and the badges that were no longer permitted were destroyed. This matter is still in-progress, as the final step to close the complaint includes a requirement that the contractor's security personnel complete training on how to safeguard PII.

U.S. Customs and Border Protection (CBP)

COMPLAINT: An anonymous complainant wrote that, due to his citizenship, he should not have been subjected to biometric screening. The complainant said that an officer shouted at him, and threatened to deny him from boarding a flight unless he provided his fingerprints. The complainant agreed to have his fingerprints taken because he did not want to miss his flight. However, the complainant believes the officer violated regulations, and complained that the officer was aggressive, condescending, and ignorant of proper screening rules.

DISPOSITION: The CBP INFO Center sent the anonymous complaint to the district field office for review and possible training. The complainant was correct that, based on his citizenship, he is exempt from biometric screening upon entering the U.S. for tourism. As the complaint was anonymous, the CBP INFO Center was not able to reply to the complainant directly.

U.S. Immigration and Customs Enforcement (ICE)

COMPLAINT: ICE Privacy received a complaint from an employee who alleged that his supervisor was instructing a detailee in his office to operate outside the scope of the detailee's assigned duties by handling forms that contain employee Sensitive PII. The employee further alleged that the detailee did not have a need to know the PII contained within the forms.

DISPOSITION: ICE Privacy contacted the program office and determined that the detailee's actions were within scope of his duties, as assigned by his supervisor. ICE Privacy found that the detailee did have an official need to know the PII contained in the forms. Therefore, ICE Privacy determined that no violation of privacy law or policy had occurred.

V. CONCLUSION

As required by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, as amended, this semiannual report for FY16 summarizes the Privacy Office's activities from October 1, 2015 – March 31, 2016. The Privacy Office will continue to work with Congress, colleagues in other federal departments and agencies, and the public to ensure that privacy is protected in our homeland security efforts.