Department of Homeland Security

Privacy Office

Fiscal Year 2016 Semiannual Report to Congress

For the period April 1 – September 30, 2016

January 17, 2017

Homeland Security

FOREWORD

January 17, 2017

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 April 1 – September 30, 2016.[1]

Highlights

During the reporting period, the Privacy Office:

- 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.[2]
- Partnered with the DHS Screening and Coordination Office and the National Protection and Programs Directorate 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 DHS 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.
- Issued two major reports to the White House and Congress:
  - *2016 Annual Report to Congress*
  - *2016 Privacy and Civil Liberties Report*

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

[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] Cybersecurity Act of 2015, Pub. L. No. 114-113, Division N §§ 101 - 111, 129 Stat. 2242, 2942 (2015).

across the Department. The Privacy Office undertakes these statutory and policy-based responsibilities in collaboration with DHS Component privacy[3] 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.

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,

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

[3] 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.

Pursuant to congressional notification requirements, the Privacy Office provides this report to the following Members of Congress:

The Honorable Michael Pence
President, U.S. Senate

The Honorable Paul D. Ryan
Speaker, U.S. House of Representatives

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

The Honorable Claire McCaskill
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 Dianne Feinstein
Ranking Member, U.S. Senate Committee on the Judiciary

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

The Honorable Mark Warner
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*,[4] 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."

[4] 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, privacy 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*,[5] the *Homeland Security Act of 2002*,[6] and DHS policy;
3. System of Records Notices, as required under the *Privacy Act of 1974*, and any associated Final Rules for Privacy Act exemptions;[7]
4. Privacy Act Statements, as required under the Privacy Act,[8] to provide notice to individuals at the point of collection;
5. Computer Matching Agreements, as required under the Privacy Act;[9]
6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*;[10]
7. Privacy Compliance Reviews, per the authority granted to the Chief Privacy Officer by the *Homeland Security Act of 2002*;[11]
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[12] (ITAR); and
10. Other privacy reviews, such as implementation reviews for public-facing information sharing agreements.

---

[5] 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.

[6] 6 U.S.C. § 142.

[7] 5 U.S.C. §§ 552a(e)(4), (j), (k). *See also* OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act", *available at*: https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a108/omb_circular_a_108_12_12_16.pdf, 81 Fed. Reg. 94424 (Dec. 23, 2016), available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf. .

[8] 5 U.S.C. § 552a(e)(3).

[9] 5 U.S.C. § 552a(o)-(u).

[10] 42 U.S.C. § 2000ee-3.

[11] 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.

[12] 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:** ***April 1 – September 30, 2016***	
Type of Review	***Number of Reviews***
Privacy Threshold Analyses	486
Privacy Impact Assessments	33
System of Records Notices and associated Privacy Act Exemptions	8
Privacy Act (e)(3) Statements	24
Computer Matching Agreements	1
Data Mining Reports	0
Privacy Compliance Reviews	0
Privacy Reviews of IT and Program Budget Requests[13]	0
Information Technology Acquisition Reviews[14] (ITAR)	396
Other Privacy Reviews	0
Total Reviews	***948***

[13] The DHS Office of 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, *except for this reporting period since the number is not yet available.*
[14] 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 September 30, 2016, 90 percent of the Department's FISMA systems that require a PIA had an applicable PIA. During the reporting period, the Office published 33 PIAs: 10 new and 23 updated.

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

Here is a summary of significant PIAs published during the reporting period, along with a hyperlink to the full text.

New Privacy Impact Assessments

DHS/ALL/PIA-055 DHS Data Analysis Tools *(August 08, 2016).*
The Office of Intelligence and Analysis (I&A) is developing, deploying, and using Data Analysis Tools (DAT) to perform enhanced analysis of DHS data sets and other data sources available to DHS in support of its homeland security mission. This PIA examines the privacy implications of DATs, as they will analyze data sources that contain PII. It describes the types of tools the Department may develop, how the tools will use data, what information the tools will use, how information is protected when it is used in DATs, and the oversight process for DAT deployment. Additionally, this PIA describes a prototyping environment on the classified DHS network that I&A will use to facilitate the development and testing of DATs.

DHS/CBP/PIA-030 Departure Information Systems Test *(June 12, 2016).*
U.S. Customs and Border Protection (CBP) will operate the Departure Information Systems Test in order to identify reliable and cost-effective border management capabilities that can be deployed nationwide and across multiple modes of travel. The Test will seek to test CBP's ability to verify the biometrics of departing travelers. Photos of travelers taken during boarding will be compared against photos taken previously (U.S. passport, U.S. visa, and other DHS encounters) and stored in existing CBP systems. Prior to the departure of each flight, CBP will collect facial images and boarding pass information of all travelers, including U.S. citizens, as they pass through the passenger loading bridge to board their flight. CBP will use this data to test the ability of CBP data systems to confirm a traveler's identity using a facial biometric comparison as the traveler departs from the United States.

DHS/CBP/PIA-033 Electronic Visa Update System (EVUS) *(September 12, 2016).*
CBP's Electronic Visa Update System (EVUS) is a web-based enrollment system used to collect information from nonimmigrant aliens who 1) hold a passport that was issued by an identified country approved for inclusion in the EVUS program; and 2) have been issued a U.S. nonimmigrant visa of a designated category. EVUS collects updated information in advance of an individual's travel to the United States. EVUS also enables DHS to collect updated information from designated travelers during the interim period between visa applications. CBP published this PIA because EVUS is a new

system that will collect and use PII from individuals who meet the EVUS programmatic criteria, as well as information from U.S. citizens identified on the EVUS enrollment request.

DHS/FEMA/PIA-041 Operational Use of Publicly Available Social Media for Situational Awareness *(April 22, 2016).*
The Federal Emergency Management Agency (FEMA), Office of Response and Recovery (ORR), has 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). 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. While this initiative is not designed to actively collect PII, FEMA conducted this PIA because FEMA's Watch Centers may collect, maintain, and disseminate limited amounts of PII in extremis situations to prevent the loss of life or serious bodily harm.

DHS/NPPD/PIA-030 Continuous Diagnostics and Mitigation (CDM) *(September 30, 2016).*
The National Protection and Programs Directorate (NPPD) Office of Cybersecurity and Communications (CS&C) developed the Continuous Diagnostics and Mitigation (CDM) program to support government-wide and agency-specific efforts to implement adequate, risk-based, and cost-effective cybersecurity. CDM provides continuous monitoring, diagnostics, and mitigation services designed to strengthen the security posture of participating federal civilian departments and agencies' systems and networks through the establishment of a suite of capabilities that enables network administrators to know the state of their respective networks at any given time, informs Chief Information Officers (CIO) and Chief Information Security Officers (CISO) on the relative risks of threats, and makes it possible for government personnel to identify and mitigate vulnerabilities. This PIA is being conducted to cover Phase One, Two, and Three of the program and addresses privacy risks associated with CS&C's deployment and operation of the CDM Federal Dashboard.

Updated Privacy Impact Assessments

DHS/CBP/PIA-021 TECS System: Platform *(August 12, 2016).*
CBP owns and operates the TECS (not an acronym) system. The TECS Platform facilitates information sharing among federal, state, local, and tribal government agencies, as well as with international governments and commercial organizations. Through the TECS Platform, users are able to input, access, or maintain law enforcement, inspection, intelligence-gathering, and operational records. CBP published this PIA as a complement to the previously published DHS/CBP/PIA-009, CBP Primary and Secondary Processing PIA from 2010, to provide notice to the public and to assess the privacy risks and mitigations associated with the TECS Platform.

DHS/CBP/PIA-010(a) – Analytical Framework for Intelligence (AFI) *(June 1, 2012, 2016, updated and published September 01, 2016).*
CBP's Analytical Framework for Intelligence (AFI) system provides enhanced search and analytical capabilities to identify, apprehend, and prosecute individuals who pose a potential law enforcement or security risk, and aids in the enforcement of customs, immigration, and other laws enforced by DHS at the border. Since the original PIA, CBP has increased technical safeguards in AFI; added a new user role, additional DHS users, and additional data sources; and developed a governance process that

includes the operational and oversight components of CBP. CBP updated the original AFI PIA to address recommendations from the DHS Privacy Office contained in a Privacy Compliance Review on AFI, and to promote transparency regarding the new users, data sources, data access, and analytic functions of AFI.

DHS/ICE/PIA-001(b) Student and Exchange Visitor System Admissibility Indicator (SEVIS-AI) *(June 23, 2011, updated and republished July 19, 2016).*
The Student and Exchange Visitor Information System (SEVIS), owned and operated by U.S. Immigration and Customs Enforcement (ICE), Student and Exchange Visitor Program (SEVP), is an Internet-based system that maintains real-time information on nonimmigrant students and exchange visitors, their dependents, and the approved schools and designated U.S. sponsors that host these nonimmigrants. The original PIA for SEVIS was published on February 5, 2005. This update provides notice of ICE's implementation of a new method to routinely share SEVIS information with U.S. Customs and Border Protection (CBP) to assist CBP at primary inspection points with information on admissibility for nonimmigrants seeking to enter the United States in the F, M, and J classes of admission.

DHS/NPPD/PIA-027(a) EINSTEIN 3 Accelerated *(April 19, 2013, updated and republished May 06, 2016).*
NPPD conducted this PIA Update to describe the addition of a new intrusion prevention security service, known as Web Content Filtering (WCF), to the EINSTEIN 3 Accelerated (E^3A) program. WCF 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. This service will be added to the existing E^3A intrusion prevention security services that are already in place, as described in the original E^3A PIA, published April 19, 2013.

DHS-USCIS-PIA-013(a) Fraud Detection and National Security Data System *(May 18, 2016).*
United States Citizenship and Immigration Services (USCIS) developed the Fraud Detection and National Security Data System (FDNS-DS) as the primary case management system used to record requests and case determinations involving immigration benefit fraud, public safety, and national security concerns. Since its initial deployment, USCIS has incorporated a new screening functionality into FDNS-DS, known as ATLAS, to more effectively identify and review cases involving fraud, public safety, and national security concerns. USCIS updated and reissued the entire FDNS-DS PIA, originally published on June 29, 2008, to capture these updates.

System of Records Notices

The Department publishes System of Records Notices (SORN) consistent with the requirements outlined in the *Privacy Act of 1974*.[15] 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 September 30, 2016, 99 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the Office published 10 SORNs: 4 new and 6 updated.

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.

Here is a summary of significant SORNs published during the reporting period, along with a hyperlink to the full text in the *Federal Register*.

New System of Records Notices

DHS/FEMA-013 Operational Use of Social Media for Situational Awareness Initiative
This system of records authorizes FEMA to monitor, collect, and maintain information from publicly available social media sources to provide critical situational awareness in support of FEMA's mission to reduce the loss of life and property and protect the nation from all hazards, including natural disasters, acts of terrorism, and other man-made disasters. FEMA's social media monitoring initiative was neither designed nor intended to collect PII; however, given the unpredictable nature of disasters and emergency management, the content that is posted, and the voluntary and unrestricted nature of social media, it is possible for FEMA to collect, maintain, and in extremis circumstances, disseminate a limited amount of PII to first responders. FEMA published this SORN because FEMA may collect PII from social media for certain narrowly tailored categories. For example, in the event of an in extremis situation involving potential life and death, FEMA will collect and share certain PII with federal, state, local, tribal, and territorial first responders in order for them to take the necessary actions to save a life, such as the name and location of a person asking for help during a man-made or natural disaster. *(81 Fed. Reg. 23503, April 21, 2016)*

Updated System of Records Notices

DHS/ALL-30 Use of the Terrorist Screening Database
This system of records allows 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 is reducing the number of claimed exemptions, pursuant to a concurrently published Final Rule elsewhere in the Federal Register. A detailed description of the recent changes to

[15] 5 U.S.C. §§ 552a(e)(4), (j), (k). *See also* OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act", *available at*: https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a108/omb_circular_a_108_12_12_16.pdf, 81 Fed. Reg. 94424 (Dec. 23, 2016), available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf. .

the DHS/ALL-030 Use of the Terrorist Screening Database (TSDB) System of Records is published elsewhere in the Federal Register at 81 FR 3811 (Jan. 22, 2016). *(81 Fed. Reg. 19988, April 6, 2016)*

- Final Rule: DHS issued a final rule to amend its regulations to exempt portions of an existing system of records titled, "DHS/ALL-030 Use of the Terrorist Screening Database System of Records" from certain provisions of the Privacy Act. Specifically, the Department exempts portions of the "DHS/ALL-030 Use of the Terrorist Screening Database System of Records" from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements. (*81 Fed. Reg. 19988, April 6, 2016)*

DHS/CBP-009 Electronic System for Travel Authorization (ESTA)

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 or Form I-94W information against selected security and law enforcement databases at DHS, including TECS (not an acronym) and the Automated Targeting System (ATS). In addition, ATS retains a copy of ESTA application and Form I-94W data to identify individuals from Visa Waiver Program countries who may pose a security risk to the United States. The ATS maintains copies of key elements of certain databases in order to minimize the impact of processing searches on the operational systems, and to act as a backup for certain operational systems. DHS may also vet ESTA application information against security and law enforcement databases at other federal agencies to enhance DHS's ability to determine whether the applicant poses a security risk to the United States, and is eligible to travel to and enter the United States under the VWP. The results of this vetting may inform DHS's assessment of whether the applicant's travel poses a law enforcement or security risk and whether the application should be approved. CBP updated this SORN, last published on June 17, 2016, to clarify the category of individuals, expand a routine use, and expand the record source categories to include information collected from publicly available sources, such as social media. *(81 Fed. Reg. 60713, September 02, 2016)*

DHS/ICE-014 Homeland Security Investigations Forensic Laboratory (HSI-FL)

The HSI-FL is a U.S. crime laboratory specializing in scientific authentication; forensic examination; research, analysis, and training related to travel and identity documents; latent and patent finger and palm prints; and audio and video files in support of law enforcement investigations and activities by DHS and other agencies. As a result of a biennial review of this system, DHS/ICE is updating this system of records notice to include minor changes that were made to make the wording consistent with the routine uses of other ICE SORNs, and in accordance with Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act.[16] ICE made minor changes to 1) Routine Use G that supports ICE's sharing of information with domestic and international law enforcement agencies when there is a violation, or potential criminal, civil, or regulatory violation of law, rule, regulation, or order; 2) Routine Use H that supports parties involved in court litigation when DHS is a party or has an interest; 3) Routine Use V that supports DHS in making a determination regarding redress for an individual; and the retention and disposal section has been updated to note that the current approved ICE records disposition authority states that all case files, other than war crime cases, be destroyed five years after the date of completion of the forensic examination. War crime cases are unscheduled at this time, and thus deemed permanent records. In addition, a new schedule is currently being reviewed and once approved will provide lengthier

[16] OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act", *available at*: https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a108/omb_circular_a_108_12_12_16.pdf, 81 Fed. Reg. 94424 (Dec. 23, 2016), available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf.

retention periods than the current schedule. ICE is proposing that case files related to significant cases such as war crimes, terrorism, and homicide cases should be retained at ICE for 20 years after completion of the investigation and all actions based thereon, and then transferred to the National Archives for permanent retention. Once the schedules are approved the SORN will be updated to reflect the changes. The exemptions for the existing SORN will continue to be unchanged. *(81 Fed. Reg. 45523, July 14, 2016)*

Privacy Compliance Reviews

The DHS Privacy Office serves as both an advisor and oversight body for the Department's privacy-sensitive programs and systems. The Privacy Compliance Review (PCR) was designed as a collaborative effort to help improve a program's ability to comply with existing privacy compliance documentation, including Privacy Impact Assessments (PIA), System of Records Notices (SORN) and/or formal agreements such as Memoranda of Understanding or Memoranda of Agreements. A PCR may result in a public report or internal recommendations, depending upon the sensitivity of the program under review.

The Office did not publish any PCRs during this reporting period. However, the Privacy Office completed Framework Guidance for conducting Privacy Compliance Reviews.

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

Additional Reporting

***2016 Privacy Office Annual Report*:** In November 2016, the DHS Privacy Office published its Annual Report to Congress, highlighting the achievements of the Privacy Office for the period July 2015 - June 2016. All Annual Reports are available on the Privacy Office website, www.dhs.gov/privacy, under Privacy & FOIA Reports.

2016 Privacy and Civil Liberties Assessment Report: Executive Order 13636[17] (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 DHS Privacy Office and the Office for Civil Rights and Civil Liberties (CRCL). In July 2016, the Privacy Office published the 2016 Report. Additional reports are available on the Privacy Office website, www.dhs.gov/privacy, under Cybersecurity and Privacy.

[17] https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

II. ADVICE AND RESPONSES

The Privacy Office provides significant ongoing privacy policy leadership on a wide range of topics in various fora. Highlights are summarized below.

Privacy Policy

- Collaborated with NPPD's Office of Privacy to fulfill DHS's requirement under the Cybersecurity Information Sharing Act of 2015 (CISA) 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 CISA.[18]
- Partnered with the DHS Screening and Coordination Office and NPPD's Office of Privacy 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 DHS 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.

[18] Cybersecurity Act of 2015, Pub. L. No. 114-113, Division N §§ 101 - 111, 129 Stat. 2242, 2942 (2015).

III. Training and Outreach

Mandatory Online Training

157,058 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.

4,850 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

2,993 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.
- Annual Privacy Compliance Workshop: Each year, over 200 privacy professionals from over 40 federal agencies attend this workshop to hear DHS privacy experts convey privacy compliance best practices.
- 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: Upon request or as needed, the Privacy Office provides customized 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

- International Association of Privacy Professionals (IAPP) Global Privacy Summit – In April 2016, in Washington, DC, the Acting Chief Privacy Officer participated in a panel discussion, *Reworking Privacy Management within the Federal Government*.
- Meetings with Canadian Officials – In April 2016, the former Chief Privacy Officer traveled to Ottawa, Canada to meet with senior government officials 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.
- Meeting of the American Bar Association's Cybersecurity, Data Protection and Privacy Committee In May 2016, the former Chief Privacy Officer participated in a panel discussion on the Cybersecurity Information Sharing Act of 2015 and related Privacy and Civil Liberties Guidelines.
- American Society of Access Professional's National Training Conference – In July 2016, the Acting Chief Privacy Officer participated in a panel discussion, *Flex your Privacy Muscle: How to Strengthen your Privacy Program.*
- 11th Annual Homeland Security Law Institute – In August 2016, the Acting Chief Privacy Officer participated in a panel discussion, *A Challenge for All: Preserving Privacy & Ensuring Data Security*.

Component Training and Outreach

Federal Emergency Management Agency (FEMA)

- Supported FEMA'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 Privacy Point of Contact at each disaster site 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 (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 as well as privacy incident reporting and mitigation.
- Served on the agency's Intranet Governance Working Group to establish governance on FEMA's use of SharePoint, specifically with respect to safeguarding PII.
- Served on the agency's Information Technology Acquisition Review board for to address privacy risks and ensure appropriate cyber hygiene clauses are incorporated into FEMA's contracts.

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.
- Provided Privacy Awareness 101 Training to 23 Federal Protective Service FOIA liaisons from all 11 regions in Atlanta, Georgia.
- Senior Privacy Officer participated in a panel discussion entitled, *Focus on Privacy Requirements and Cybersecurity*, at the Dixon Hughes Goodman 21st Annual Government Contracting Update.
- Hosted the Washington, D.C. Metropolitan Police Department's Privacy Officer, who discussed the impact of body cameras on privacy.
- Deputy Privacy Officer presented on *Embedding Privacy into the IT Acquisition Process* at the Annual DHS Privacy Compliance Workshop. The focus of this presentation was on the importance of ensuring the appropriate privacy provisions and clauses are inserted into contracts and statements of work where contractors have access to PII.
- Senior Privacy Officer presented at the Federal Privacy Council sponsored "Tech Tuesday" on *Privacy Considerations in Federated Identity Management*.
- Senior Privacy Analyst participated on a panel at the American Bar Association's 11th Annual Homeland Security Law Institute event, *The Cybersecurity Act of 2015 – An Overview and Update*.
- Hosted the DHS Science and Technology Directorate's Privacy Officer for an event titled, *Pokémon WAIT*, to discuss privacy considerations in the latest trends in social media, apps, and mobile gaming.
- From April-September, the NPPD Deputy Privacy Officer participated in numerous speaking engagements on DHS's implementation of CISA, and the development of the Privacy and Civil Liberties Guidelines. These events included a briefing for all of the federal Privacy and Civil

Liberties Officers, a webinar for sector-specific agencies, a DHS-hosted public workshop, and two conferences for corporate counsels participating in cyber information sharing.
- Senior Privacy Officer presented on *Building Privacy into Cyber Threat Information Sharing*, at the California Cyber Summit in Sacramento, California.
- Published two issues of the quarterly newsletter, *NPPD Privacy Update*, which is distributed NPPD-wide and posted on the NPPD Office of Privacy internal 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 NPPD's Privacy Day on *Augmenting Reality Apps and Privacy Risks.*

United States Citizenship and Immigration Services (USCIS)

- Trained over 150 individuals located in three international districts on information sharing, protection of PII, and the reporting of privacy incidents.
- Provided instructor-led training on *Privacy Incident Response* to records managers and other records personnel to ensure compliance with USCIS' and DHS requirements to report privacy incidents.
- Trained staff in the Forms Management Branch on the privacy requirements for the forms review process, and the role of the USCIS Privacy Office in the form process.
- Trained the FDNS Data Science Working Group on privacy compliance.
- Developed a privacy module for the Information Sharing Journeyman Course to convey the USCIS and DHS privacy requirements for information sharing.
- Hosted a Lunch & Learn educational session during tax season to provide valuable tips on how to prevent identity theft.
- Provided a Privacy Overview Briefing to the New Central Region Field Office Director.
- Revised the USCIS internal web infrastructure to more effectively communicate privacy information to the USCIS workforce.
- Briefed program offices on USCIS privacy policies relating to privacy compliance, how to safeguard PII, requirements for Computer Readable Extracts (CRE), and other privacy-related policies.
- Provided training to Office of the Chief Counsel Service Center Law Division paralegals on privacy requirements related to their duties.
- Monitored and reviewed multiple IT projects through the agile development process. As a result, checkpoints for privacy have been built into the project development process so that the project

developers and the Privacy Office quickly identify privacy issues and, if needed, halt production that may pose undue privacy problems.
- Published the USCIS Office of Privacy quarterly newsletter, entitled *Privacy Chronicles*, to promote privacy awareness across USCIS, reiterating the importance of working together as partners to ensure that privacy is incorporated into all USCIS policies, guidance, and procedures.
- Implemented a digital signage campaign to promote private awareness. A new tip is displayed each quarter on all monitors in USCIS HQ facilities.
- Broadcast a quarterly reminder memorandum from the USCIS Privacy Officer to all USCIS employees, reminding staff of their responsibility to protect PII.
- Sent the annual thank you letter from the USCIS Privacy Officer to all USCIS supervisors, expressing gratitude for exemplary leadership in promoting privacy awareness within their respective offices.
- Hosted an Ice Cream Social at which privacy staff discussed privacy concerns and answered questions. Privacy brochures were distributed:
    - *Privacy At Home*, provides tips for individuals to protect their personal information from identity theft.
    - *Sensitive PII FAQs*, provides guidelines on how to protect Sensitive PII and identify the differences between PII and Sensitive PII.
- Held an agency-wide Privacy Contest, where the USCIS Office of Privacy asked for program offices to submit a written explanation of what has been done to promote privacy within their offices.

U.S Customs and Border Protection (CBP)

- Provided six training sessions in Laredo, Texas, which included all CBP operational components as well as attendees from ICE. The trainings included real-life examples to allow the audience to better understand how privacy interplays in their day-to-day work.
- Presented an in-depth session on how to mitigate privacy incidents at the American Society of Access Professionals, National Training Conference.
- Collaborated with the Office of Information Technology to refresh the privacy section of the 2017 IT Computer Security Awareness and Rules of Behavior Training.

U.S. Immigration and Customs Enforcement (ICE)

- ICE's Assistant Director for Information Governance & Privacy spoke on *Re-working Privacy Management within the Federal Government* at the IAPP Global Privacy Summit on April 6, 2016.

United States Secret Service (USSS)

- Hosted a Privacy Awareness Day event entitled, "Privacy Wheel of Information" to educate employees and contractors on best privacy practices and federal privacy laws.
- Trained 264 new Special Agents and 216 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.[19]

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[20]	In Progress (Current Period)	In Progress (Prior Periods)
Process & Procedure	0	2	0	2
Redress	184	184	0	0
Operational	1,123	1,156	21	1
Referred	1	1	0	0
Total	1,308	1,343	21	3

.

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.[21]
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.

[19] *See* DHS Privacy Policy Guidance Memorandum 2007-01/Privacy Policy Directive 262-12, *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.

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

[21] 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: The NPPD Office of Privacy received a complaint from personnel regarding the process in which an NPPD contractor was collecting PII from federal employees. The contractor issued identification badges to federal employees so that they may access the contractor's offsite facility for reviews of deliverables and training opportunities.

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. Lastly, the NPPD Office of Privacy provided in-person Privacy Awareness/Safeguarding PII training to all of the contractor security office personnel on April 27, 2016, and held a follow up meeting with the COR and the Security Officer to close this matter.

U.S. Customs and Border Protection (CBP)

COMPLAINT: An anonymous complainant arriving at a Port of Entry was sent for secondary inspection. The complainant felt that they were treated like a second-class citizen. While waiting in secondary, the complainant witnessed a woman with an infant being chastised by a CBP Officer for standing just outside of the waiting room while trying to calm the infant's crying. The complainant also witnessed one other passenger being treated rudely by a CBP officer for not moving fast enough,

with the insinuation that it was racially motivated due to the traveler being a different race than the CBP Officer. The complainant expressed concerns over how CBP treats foreigners and minorities.

DISPOSITION: The CBP INFO Center found that there was insufficient information regarding date, time, flights, or names of CBP Officers involved. As this was an anonymous complaint, the CBP INFO Center can only act on the information provided, and no contact information was provided by the complainant to obtain additional information and details regarding the alleged incident. This complaint was mentioned in meetings with the CBP Office of Field Operations, so that they can provide additional sensitivity training to CBP staff.

COMPLAINT: A complainant arrived at Port of Entry and was sent to secondary inspection. The complainant, who is female, was sent to two male CBP officers despite there being female officers available at the time. The complainant claims the CBP Officers went through her belongings and spoke to her in a threatening tone, stating that they had the power to send the complainant back to her home country. The complainant stated that the officer then made remarks about her physical appearance, and expressed concerns about the officers being sexist.

DISPOSITION: The CBP INFO Center processed the complaint and sent a response directly back to the complainant. The response apologized for the unpleasant experience, and explained CBP's search authority, the secondary process, and mission to protect the Homeland. It also explained that it is not the intent of CBP to subject travelers to unwarranted scrutiny, but there are procedures in place to determine admissibility that unfortunately inconvenience law-abiding citizens at times in order to detect those that are involved in illicit activities. Also, the letter explained that CBP uses diverse factors to refer individuals for examination, and there are instances when an officer's best judgment might turn out to be unfounded. Finally, the letter stated that CBP offers any traveler the opportunity to speak with a supervisor to address any comments or concerns raised during the inspection process, that all allegations of unprofessional conduct by any of its employees are taken seriously, and that CBP appreciated the complainant's initiative in bringing this matter to its attention. Additionally, the complaint was forwarded to the CBP Office of Professional Responsibility (OPR) for investigation, as well as to the Prevention of Sexual Assault (PREA) coordinator for investigation, due to the nature of the allegations.

U.S. Immigration and Customs Enforcement (ICE)

COMPLAINT: ICE Privacy received a complaint from an employee who alleged that his supervisor emailed his Social Security number (SSN) in the body of an email to multiple other employees within the same office. The employee further alleged that these employees did not have a need to know his SSN.

DISPOSITION: ICE Privacy contacted the supervisor and determined that the employees within the office already had access to each other's SSNs in the course of their official duties. Because the supervisor had sent the email containing the SSNs in the course of his official duties, ICE Privacy determined that no Privacy Act or privacy policy violation occurred. ICE Privacy also determined that this issue will not occur in the future because the office's business process has changed so that SSNs will no longer be shared in this manner.

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 April 1, 2016 – September 30, 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.