
# Department of Homeland Security

## Privacy Office

## Fiscal Year 2018 Semiannual Report to Congress

*For the period October 1, 2017 – March 31, 2018*

*July 25, 2018*

Homeland Security

# FOREWORD

*July 25, 2018*

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's Fiscal Year 2018 Semiannual Report to Congress, covering the time period October 1, 2017 – March 31, 2018.[1]

## Highlights

During the reporting period, the Privacy Office:

- Completed 774 privacy reviews, including 541 Privacy Threshold Analyses, 22 Privacy Impact Assessments, five System of Records Notices, and three Privacy Compliance Reviews.
- Published its *2017 Annual Report to Congress*.
- Issued one new and two revised Privacy Policy Instructions on privacy incident prevention and response.

## About the Privacy Office

The *Homeland Security Act of 2002* charges the DHS Chief Privacy Officer with primary responsibility for ensuring that privacy 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.

Please direct any inquiries about this report to the Office of Legislative Affairs at 202-447-5890 or privacy@dhs.gov, or consult our website: www.dhs.gov/privacy.

[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 cover the following time periods: April – September and October – March.

[2] DHS Components have a Privacy Officer and other DHS offices have a Privacy Point of Contact. A complete list can be found here: http://www.dhs.gov/privacy-office-contacts.

Sincerely,

Philip S. Kaplan
Chief Privacy Officer
U.S. Department of Homeland Security

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

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

**The Honorable 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 Trey Gowdy**
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 Jerry Nadler**
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 2018
# 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, 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*,[4] the *Homeland Security Act of 2002*,[5] 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;[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
10. Other privacy reviews, such as implementation reviews for 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(e)(4), (j), (k). *See also* OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act", 81 Fed. Reg. 94424 (Dec. 23, 2016), available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf.
[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 exercise 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 an 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, 2017 – March 31, 2018*

| *Type of Review* | *Number of Reviews* |
|---|---|
| Privacy Threshold Analyses | 541 |
| Privacy Impact Assessments | 22 |
| System of Records Notices and associated Privacy Act Exemptions | 5 |
| Privacy Act (e)(3) Statements[12] | 17 |
| Computer Matching Agreements | 1 |
| Data Mining Reports | 0 |
| Privacy Compliance Reviews | 3 |
| Privacy Reviews of IT and Program Budget Requests[13] | 0 |
| Information Technology Acquisition Reviews[14] (ITAR) | 185 |
| Other Privacy Reviews | 0 |
| ***Total Reviews*** | ***774*** |

[12] This total does not include all Components; several are permitted to review and approve their own Privacy Act statements by the DHS Privacy Office.
[13] The Chief Information Office prepares an annual privacy score as part of its Office of Management and Budget Exhibit 300 reporting. Reviews for this category are reported only during the second semi-annual reporting period.
[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 March 31, 2018, 97 percent of the Department's Federal Information Security Modernization Act (FISMA) systems that require a PIA had an applicable PIA. During the reporting period, the Office published 22 PIAs: 12 new and 10 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-063 Drug-Free Workplace Program *(January 2, 2018)*
The DHS Office of the Chief Human Capital Officer (OCHCO) oversees the departmental Drug-Free Workplace (DFW) program, and developed and implemented a comprehensive DFW program that includes the Components developing their own DFW plans that conform to DHS policies. This PIA outlines the collection and use of the personally identifiable information (PII) of current employees and applicants who are selected for employment at DHS, who are subject to the requirements of the DHS DFW program.

DHS/CBP/PIA-049 CBP License Plate Reader Technology *(December 11, 2017)*
U.S. Customs and Border Protection (CBP) uses a combination of surveillance systems, including license plate reader technology, to provide comprehensive situational awareness along the United States border to assist CBP in detecting, identifying, apprehending, and removing individuals illegally entering the United States at and between ports of entry or otherwise violating United States law. License plate reader technology includes commercially available technologies such as fixed and mobile license plate readers. CBP conducted this PIA to provide public notice of this CBP-owned and operated technology, assess the privacy risks, and describe the steps CBP is taking to mitigate them.

DHS/CBP/PIA-051 Automated Passport Control (APC) and Mobile Passport Control (MPC) *(March 19, 2018)*
CBP developed the Automated Passport Control (APC) and Mobile Passport Control (MPC) programs to automate and expedite eligible travelers' entry process into the United States. These programs enable travelers to perform select entry declaration and inspection requirements tasks through a self-service kiosk (APC) or a mobile device application (MPC). DHS conducted this PIA because APC and MPC collect PII from members of the public.

DHS/FEMA/PIA-049 Individual Assistance (IA) Program *(January 11, 2018)*
The Federal Emergency Management Agency (FEMA) Individual Assistance (IA) program provides disaster recovery assistance to individuals and supports FEMA's recovery mission under the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended (Stafford Act), through the collection and processing of disaster survivor information obtained through electronic or paper-based means. FEMA published this PIA to broadly cover the collection, use, maintenance, retrieval, and dissemination of PII of applicants for the purpose of implementing the FEMA IA programs.

DHS/USCG/PIA-026 USCG Research and Development Center (RDC) Small Unmanned Aircraft Systems (sUAS) Program *(February 22, 2018)*
The United States Coast Guard (USCG) Research and Development Center (RDC) has been tasked and funded to evaluate small Unmanned Aircraft Systems (sUAS) for potential use by USCG for operational missions. sUAS include small aircraft (typically less than 55 pounds in weight) that are generally operated using a wireless ground control station (GCS). The aircraft are equipped with sensors and cameras that can capture images and transmit them to standalone GCSs to provide aerial views of USCG missions for situational awareness to the operators and users. USCG conducted this PIA to address the privacy impact of sUAS surveillance and image capturing capabilities.

## Updated Privacy Impact Assessments

DHS/ALL/PIA-052(a) DHS Insider Threat Program *(March 1, 2018)*
The Insider Threat Program (ITP) manages insider threat matters within DHS. The ITP was mandated by Executive Order (EO) 13587, ''Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,'' issued October 7, 2011. The EO requires all federal agencies that operate or access classified computer networks to establish an insider threat detection and prevention program covering all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the Federal Government) to ensure the security of classified networks and the responsible sharing and safeguarding of classified information on those networks with appropriate protections for privacy and civil liberties. Insider threats include: attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities directed against the Department and its personnel, facilities, resources, and activities; unauthorized use of or intrusion into automated information systems; unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary information or technology; and indicators of potential insider threats. The DHS ITP monitors activity on all three DHS networks: Unclassified (A-LAN), SECRET (B-LAN also known as the Homeland Secure Data Network), and TOP SECRET (C-LAN also known as the Joint Worldwide Intelligence Communications System). DHS updated this PIA to reflect the application of the insider threat program to all networks.

DHS/CBP/PIA-008(a) CBP Border Searches of Electronic Devices (*January 4, 2018*)
CBP published an updated PIA to provide notice and a privacy risk assessment of the CBP policy and procedures for conducting searches of electronic devices pursuant to its border search authority. This PIA describes recent changes to, and the reissuance of, CBP's policy directive governing border searches of electronic devices, CBP Directive No. 3340-049A, Border Searches of Electronic Devices (January 2018). CBP conducted a privacy risk assessment of this updated policy as applied to any device that may contain information in an electronic or digital form, such as computers, tablets, disks, drives, tapes, mobile phones, and other communication devices, cameras, and music and other media players. Noting the evolution of the operating environment since the 2009 Directive was issued, along

with advances in technology and other continuing developments, CBP reviewed and updated its Directive.

DHS/ICE/PIA-039(a) Acquisition and Use of License Plate Reader Data from a Commercial Service *(December 27, 2017)*
United States Immigration and Customs Enforcement (ICE) has procured query-based access to a vendor-owned commercial License Plate Reader (LPR) data service that stores recorded vehicle license plate data from cameras equipped with license plate reader technology. ICE uses LPR data from this service in support of its criminal and administrative law enforcement missions. In March 2015, ICE published a PIA announcing ICE's intention to procure access to a commercial LPR database and describing the controls ICE would put in place to ensure the agency complies with privacy and civil liberties requirements when using the service. This PIA was updated to explain ICE's operational use of the service it has procured, and describes the privacy and civil liberties protections that have been implemented by the agency and the vendor.

DHS/NPPD/PIA-020(b) Private Sector Clearance Program for Critical Infrastructure *(March 7, 2018)*
The Private Sector Clearance Program for Critical Infrastructure (PSCP) ensures that critical infrastructure private sector owners, operators, and industry representatives, specifically those in positions responsible for the protection, security, and resilience of their assets, are processed for the appropriate security clearances. With clearances, these owners, operators, and representatives can access classified information to make more informed decisions. The PSCP facilitates the processing of these security clearance applications for private sector partners, and is currently administered by the National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) Security Office. NPPD updated the PSCP PIA to account for changes to the PSCP clearance process and PSCP website.

DHS/USCIS/PIA-060(a) Customer Profile Management System *(February 2, 2018)*
United States Citizenship and Immigration Services (USCIS) developed the Customer Profile Management System (CPMS) as a person-centric repository of biometric and biographic information to support USCIS's mission to administer immigration benefits. USCIS currently shares information with various international information sharing partners in accordance with information sharing agreements that are in place between DHS and foreign governments. Until now, USCIS was only receiving and responding in an automated process to support international data sharing efforts in response to secondary queries from Canada and Australia. USCIS updated this PIA to document USCIS's automated support of DHS's biometric-based information sharing with New Zealand, in addition to previously discussed Canada and Australia. This update also describes how USCIS receives and responds to secondary queries in an automated process from New Zealand, in addition to previously discussed Canada and Australia.

## *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 assessments to ensure that all SORNs remain accurate, up-to-date, and appropriately scoped; that all SORNs are published in the *Federal Register*; and that all significant changes to SORNs are reported to the Office of Management and Budget (OMB) and Congress.

As of March 31, 2018, 100 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the Office published five SORNs: three new and two updated. DHS published no Privacy Act rulemakings within this time period.

All DHS SORNs, Privacy Act 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/ALL-040 DHS Personnel Recovery Information System

The DHS Personnel Recovery Programs are responsible for: (1) ensuring that DHS personnel and contractors assigned overseas or on official travel outside the continental United States have proper training and equipment to fulfill their respective mission; (2) maintaining a 24 hour monitoring center for all overseas personnel who are traveling outside their country of assignment; (3) executing a coordinated response to personnel recovery incidents; (4) maintaining a notification system within DHS to provide emergency-related notifications as needed without jeopardizing the safety of DHS personnel (including federal employees and contractors); and (5) providing and developing tracking and locating technology. This newly established system is included in the DHS's inventory of record systems. *(82 Fed. Reg. 49407, October 25, 2017)*

DHS/FEMA-014 Hazard Mitigation Planning and Flood Mapping Products and Services Records System

This new SORN describes FEMA's collection and maintenance of records on individuals who are involved in the creation and updating of flood maps, individuals requesting information on or purchasing flood map products or services, and individuals involved with hazard mitigation planning. This newly established system is included in the DHS's inventory of record systems. *(82 Fed. Reg. 49404, October 25, 2017)*

[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," 81 Fed. Reg. 94424 (Dec. 23, 2016), available at: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf.

## *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 PIAs, SORNs, 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.

- *DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews* implements DHS Directive 047-01, "Privacy Policy and Compliance," with regard to the Component Head's responsibility to assist the Chief Privacy Officer (CPO) in reviewing Component activities to ensure that privacy protections are fully integrated into Component operations.

The Privacy Office published three PCRs during this reporting period. All public PCRs are available on the Privacy Office website, www.dhs.gov/privacy, under Privacy Oversight.

Electronic System for Travel Authorization (ESTA) (*November 2017*)
CBP uses social media identifiers to vet Electronic System for Travel Authorization (ESTA) applications, as noted in the September 2016 update to the ESTA Privacy Impact Assessment (DHS/CBP/PIA-007(g)). In September of 2016, CBP began collecting, on a voluntary basis, social media identifiers from citizens and nationals of countries participating in the Visa Waiver Program (VWP) who sought to travel to the United States. The inclusion of social media identifiers on the ESTA application is the first time DHS has requested social media information as part of an application for benefits or travel to the United States. The ESTA PCR report sets forth the DHS Privacy Office's findings on CBP's compliance with the ESTA PIA and provides recommendations for best practices to protect privacy when collecting and using social media identifiers. The DHS Privacy Office found the CBP ESTA program's use of social media identifiers is compliant with the requirements outlined in the PIA, and made three recommendations to enhance privacy best practices.

DHS National Operations Center's Media Monitoring Initiative (*December 2017*)
PCRs are a key aspect of the layered privacy protections built into the DHS National Operations Center's Media Monitoring Initiative to ensure that the protections described in the PIAs are followed. The DHS Privacy Office conducted this eighth PCR to assess compliance with DHS privacy policy and the Publicly Available Social Media Monitoring and Situational Awareness Initiative PIA and SORN, as well as implementation of recommendations from previous PCRs. We found that the DHS Office of Operations Coordination, National Operations Center, continues to comply with the privacy requirements identified in privacy compliance documents, and made five recommendations to enhance privacy best practices.

USCIS Customer Profile Management Service and National Appointment Scheduling System (*October 2017*)
USCIS oversees lawful immigration to the United States. As part of this mission, USCIS receives and adjudicates requests for immigration and citizenship benefits. The administration of these benefits requires the collection of biographic and biometric information from benefit requestors. USCIS uses multiple systems to administer immigration benefits, including the Customer Profile Management Service (CPMS) and National Appointment Scheduling System (NASS). Due to the heightened privacy risks associated with the collection of biometric information, PIAs for CPMS and NASS in 2015 required the DHS Privacy Office to conduct a PCR. During the course of this PCR, the DHS

Privacy Office found USCIS to be in compliance with privacy requirements of federal privacy laws, DHS and Component privacy regulations and policies, and explicit assurances made by USCIS in existing privacy compliance documentation. We identified six recommendations designed to improve USCIS privacy compliance, and to incorporate best practices for other USCIS and DHS programs and systems.

# II. ADVICE AND RESPONSES

The Privacy Office provides privacy policy leadership on a wide range of topics in various fora, as described in detail in the *2017 Privacy Office Annual Report* cited on page one.

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

## *Privacy Policy*

In response to Office of Management and Budget (OMB) guidance issued in January 2017, *Memorandum M-17-12, Preparing for and Responding to a Breach of PII*, the Privacy Office issued one new privacy policy and two completely revised privacy policy instructions this year.

1. ***New***: *Privacy Incident Responsibilities and Breach Response Team* establishes DHS policy, responsibilities, and requirements for responding to all incidents involving PII contained in DHS information; and establishes the requirement for the Chief Privacy Officer (CPO) to convene and lead a Breach Response Team when a "major incident" involving PII has occurred,[16] or at the discretion of the CPO.
2. ***Revised***: *Privacy Incident Handling Guidance* (PIHG) establishes DHS policy for responding to privacy incidents by providing procedures to follow upon the detection or discovery of a suspected or confirmed incident involving PII in an unclassified environment.
3. ***Revised***: *Handbook for Safeguarding Sensitive PII* provides best practices and DHS policy requirements to prevent a privacy incident involving Sensitive PII during all stages of the information lifecycle: *when collecting, storing, using, disseminating, or disposing of Sensitive PII.*


[16] A breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a "major incident," as defined in OMB M-18-02. The CPO, in coordination with the Chief Information Officer (CIO) and Chief Information Security Officer (CISO), will first determine whether a privacy incident is considered a "major incident" that involves PII.

# III. Training and Outreach

## *Mandatory Online Training*

101,126 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.

1,293 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*

2,424 DHS personnel attended instructor-led privacy training courses, including the following for which the Privacy Office either sponsored or provided a trainer:

- ***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.
- ***Privacy Office Boot Camp***: The Privacy Office periodically trains new 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 FOIA staff throughout the agency responsible for processing FOIA requests.
- ***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 every six weeks to participants of this week-long training program, who represent multiple agencies.
- ***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 Briefings for Headquarters Staff*:** Upon request or as needed, the Privacy Office provides customized privacy awareness briefings to employees and contractors to increase awareness of DHS privacy policy, and convey the importance of incorporating privacy protections into any new program or system that will collect PII.

## DHS Privacy Office Outreach

Privacy Office staff present at conferences and participate in public meetings to educate and inform both the public and private sectors on DHS privacy policies and best practices.

- ***The International Association of Privacy Professionals (IAPP) Global Summit*** – On March 27 - 28, 2018, in Washington, DC, the CPO interviewed CBP's Deputy Assistant Commissioner on border security and privacy, and the Deputy CPO participated on a panel, *How to Get a Privacy Job in the Federal Government*.
- ***The Office of the Director of National Intelligence (ODNI)*** – On January 24, 2018, in McLean, Virginia, ODNI hosted a privacy seminar at which the CPO participated in a panel discussion, *Balancing Privacy and National Security: Privacy Officer Perspectives.*
- ***Federal Privacy Summit*** – On December 12, 2017, in Washington, DC, the Federal Privacy Council hosted a one-day workshop that convened privacy, technology, budget, procurement, human resources, public affairs, congressional affairs, and intergovernmental affairs staff from many federal agencies to discuss privacy and security. Subject matter experts, including the CPO and the Deputy CPO, shared best practices for protecting privacy, and ways to improve collaboration across the enterprise. Neomi Rao, Administrator, Office of Information and Regulatory Affairs at OMB gave the keynote address.

## DHS Component Privacy Office Training and Outreach

This section features proactive steps taken by DHS Component Privacy Offices to educate and inform DHS staff on privacy law and policy.

### Federal Emergency Management Agency (FEMA)

- Provided privacy awareness refresher training to the Disclosure Branch staff.
- Conducted a refresher training on how to identify and respond to privacy incidents to the FEMA Privacy Points of Contact throughout the agency.
- Provided privacy awareness refresher training to the External Affairs Division.

### National Protection and Programs Directorate (NPPD)

- Provided a Privacy Briefing during New Employee Orientation to a total of 176 new NPPD employees from all sub-components.
- Provided executive-level privacy briefings to four new Senior Executive Service employees.
- Provided Component privacy training to 38 employees and contractors for the Personnel Security Division at the Federal Protective Service (FPS).
- Provided IT Security for Privacy Professionals training as part of the Federal Privacy Council's Privacy Boot Camp.
- Provided role-based privacy training to 33 attendees during the National Cybersecurity Awareness Month "Oversharing" Webinar for both the Consumer Financial Protection Bureau and the U.S. Navy.
- Published one privacy-related article in NPPD's weekly newsletter, *NPPD Vision*, and in two issues of the quarterly newsletter, *NPPD Privacy Update.*
- NPPD's Office of Biometric Identity Management (OBIM) Section Chief participated on a panel discussion on biometrics at the 2017 Federal Privacy Council's Privacy Summit, in which she focused on how the Fair Information Practice Principles apply to biometrics.

## Transportation Security Administration (TSA)

- TSA Privacy engaged in privacy outreach with a number of advocacy groups, including the ACLU, EPIC, CDT, CATO Institute, Liberty Coalition, Privacy Coalition, and Competitive Enterprise Institute, as well as within the federal privacy community, and at the IAPP's Annual Global Privacy Summit.

## United States Citizenship and Immigration Services (USCIS)

**Training**

- Recorded a ten minute privacy overview video targeting new employees.
- Trained Information Security Officers on privacy compliance best practices, including how to draft PTAs, PIAs and SORNs.
- Provided guidance on privacy training to the Mandatory Training Advisory Committee for fiscal year 2018.
- Trained the USCIS Academy Training Center and Central Region Human, Capital and Training staff on encryption.

**Outreach**

- Participated in the "Privacy After Dark" professional networking event marking the occasion of International Data Privacy Day.
- Distributed the Central Region *Privacy Newsletter* (January, March Editions) to the entire region as well as to the Houston and Chicago Asylum offices.
- Performed outreach through the Centralized Naturalization Printing working group with regard to privacy implications inherent in the proposal process. Topics covered included compliance documentation for new systems and new forms, and privacy considerations with regard to secure mailing.
- Distributed *Privacy Tips* messaging with guidance on how to protect PII/Sensitive PII from unauthorized use and disclosure at home and at work. Privacy Tips are displayed on USCIS Connect and digital signage boards throughout the agency.
- Disseminated a monthly Internal Privacy Bulletin to inform staff of recent and upcoming privacy activities.
- Published the *Privacy Chronicles* to alert USCIS personnel of USCIS Office of Privacy news, including new employees, events and activities, and articles pertaining to breaches, social media, and hackers.

## United States Coast Guard (USCG)

- Trained new employees on the importance of protecting personal information.
- Attended Freedom of Information Act (FOIA)/Privacy Act training, "Recent Rulings in FOIA/Privacy Act Cases," sponsored by the DHS Privacy Office.

## United States Immigration and Customs Enforcement (ICE)

- Provided a Privacy Briefing during New Employee Orientation to a total of 166 new ICE employees.
- Customized and delivered 25 privacy trainings to various ICE program offices, covering topics such as privacy fundamentals, privacy incidents, and information disclosure.

- Moderated the *Getting Hired for a Privacy Job in the Federal Government* panel at the IAPP Global Privacy Summit on March 27, 2018.

## United States Secret Service (USSS or Secret Service)

- Provided FOIA/Privacy Act training to new employees at the New Employee Orientation class covering the legal requirements governing the administration of the Acts.
- Posted privacy awareness posters and flyers to encourage employees to protect privacy-sensitive records.
- Participated in a PII Working Group established by the Secret Service Director to assess the use, collection, maintenance, and safeguarding of PII.

# 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.[17]

**Table II: Type and Disposition of Complaints Received This Reporting Period**

| Complaint Type | Complaints received during the reporting period | Complaint Disposition | | |
|---|---|---|---|---|
| | | Closed, Responsive Action Taken[18] | In Progress (Current Period) | In Progress (Prior Periods) |
| **Process & Procedure** | 508 | 484 | 24 | 0 |
| **Redress** | 600 | 600 | 0 | 0 |
| **Operational** | 3520 | 3426 | 94 | 0 |
| **Referred** | 227 | 223 | 4 | 0 |
| ***Total*** | **4,855** | **4,733** | **122** | **0** |

.

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.[19]
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.
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

[17] *See* DHS Privacy Policy Guidance Memorandum 2017-01, *DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information*, available here https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

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

[19] 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.

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:

## U.S. Customs and Border Protection (CBP)

**COMPLAINT:**
A foreign traveler complained that a CBP officer at JFK Airport questioned him regarding his marital and parental status, and if he had children who stayed with him. The CBP Information Center Compliments and Complaints Branch processed the complaint and responded to the complainant. The response explained that specific laws authorize CBP staff to question travelers to determine if someone is trying to enter the U.S. unlawfully or for fraudulent purposes.

**COMPLAINT:**
A U.S. citizen traveler complained that CBP officers at Phoenix Sky Harbor Airport asked about the reason for his visit. The traveler believes the government should not ask its citizens those types of questions. He also alleged CBP officers in secondary inspection seated him within hearing distance of the questioning of another U.S. citizen with no concern for privacy. The traveler also requested an explanation of why CBP officers denied him access to an attorney. The CBP Information Center Compliments and Complaints Branch processed the complaint and responded to the complainant explaining that specific laws authorize CBP personnel to question travelers and examine merchandise coming into or leaving the United States. The response further explained that speaking with travelers is one of the ways CBP looks for illegal or prohibited items and determines whether someone is trying to enter the U.S. unlawfully or for fraudulent purposes. The traveler was also informed that individuals under arrest may have legal counsel present during the secondary inspection questioning, and advised him that the DHS Office for Civil Rights and Civil Liberties handles cases involving civil rights violations.

## Transportation Security Administration (TSA)

**COMPLAINT:**
A TSA employee complained to the TSA Privacy office that her privacy rights were violated when her leave status was published on a staff scheduling intranet site. TSA Privacy reached out to the airport's counsel, who in turn confirmed with the site administrators that the site's permissions had been corrected so that only those with a need-to-know are able to access employees' sensitive information.

# V. CONCLUSION

As required by the *Implementing Recommendations of the 9/11 Commission Act of 2007,* as amended, this semiannual report for FY18 summarizes the Privacy Office's activities from October 1, 2017 – March 31, 2018. 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.