Privacy Office

Fiscal Year 2020 Semiannual Report to Congress

Covering the period October 1, 2019 – March 31, 2020

July 23, 2020

Homeland Security

FOREWORD

July 23, 2020

I am pleased to present the *U.S. Department of Homeland Security (DHS or Department) Privacy Office's Fiscal Year 2020 Semiannual Report to Congress*, covering the period October 1, 2019 – March 31, 2020.[1]

Highlights

During the reporting period, the DHS Privacy Office:

- Completed 1,038 privacy reviews, including:
  - 674 Privacy Threshold Analyses;
  - 35 Privacy Impact Assessments; and
  - 14 System of Records Notices and associated Privacy Act Exemptions.
- Published the following congressional reports:
  - *2019 DHS Privacy Office Annual Report to Congress*
  - *2018 DHS Privacy Office Annual Data Mining Report to Congress*

About the DHS 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), as amended, the *Freedom of Information Act* (FOIA), and the *E-Government Act of 2002* require DHS to be transparent in its operations and use of information relating to individuals. The DHS Privacy Office centralizes FOIA and Privacy Act operations to provide policy and programmatic oversight and to support implementation across the Department. The DHS Privacy Office undertakes these statutory and policy-based responsibilities in collaboration with DHS Component privacy[1] 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.

Sincerely,

Dena Kozanas
Chief Privacy Officer and Chief FOIA Officer
U.S. Department of Homeland Security

[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.

[1] 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.

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

The Honorable Michael Pence
President, U.S. Senate

The Honorable Nancy Pelosi
Speaker, U.S. House of Representatives

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

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

The Honorable Lindsey Graham
Chairman, U.S. Senate Committee on the Judiciary

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

The Honorable Marco Rubio
Acting Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Mark Warner
Vice Chairman, U.S. Senate Select Committee on Intelligence

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

The Honorable Mike Rogers
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Carolyn Maloney
Chairman, Acting, U.S. House of Representatives Committee on Oversight and Reform

The Honorable James Comer
Ranking Member, U.S. House of Representatives Committee on Oversight and Reform

The Honorable Jerrold Nadler
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable Jim Jordan
Ranking Member, U.S. House of Representatives Committee on the Judiciary

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

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

DHS Privacy Office
Fiscal Year 2020
Semiannual Report to Congress

Table of Contents

LEGISLATIVE LANGUAGE

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*,[2] 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."

[2] 42 U.S.C. § 2000ee-1(f).

I. PRIVACY REVIEWS

The DHS Privacy Office is responsible for reviewing and evaluating Department programs, systems, and initiatives that either collect personally identifiable information (PII) or have a privacy impact and provide mitigation strategies, as appropriate, to reduce the privacy impact." For purposes of this report, privacy reviews include the following:

1. Privacy Threshold Analysis, as required by *DHS Privacy Policy and Compliance Directive 047-01*;
2. Privacy Impact Assessment, as required under the *E-Government Act of 2002*,[3] the *Homeland Security Act of 2002*,[4] and DHS policy;
3. System of Records Notice as required under the *Privacy Act of 1974*, as amended, and any associated Final Rules for Privacy Act exemptions;[5]
4. Privacy Act Statement, as required under the Privacy Act,[6] to provide notice to individuals at the point of collection;
5. Computer Matching Agreement, as required under the Privacy Act;[7]
6. Data Mining Report, as required by Section 804 of the *9/11 Commission Act of 2007*;[8]
7. Privacy Compliance Review, per the authority granted to the Chief Privacy Officer by the *Homeland Security Act of 2002*;[9]
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 Review;[10] and
10. Other privacy reviews at the discretion of the Chief Privacy Officer.

[3] 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*:https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2003/m03_22.pdf

[4] 6 U.S.C. § 142.

[5] 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.

[6] 5 U.S.C. § 552a(e)(3).

[7] 5 U.S.C. § 552a(o)-(u).

[8] 42 U.S.C. § 2000ee-3.

[9] 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.

[10] 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, 2019 - March 31, 2020*	
Type of Review	***Number of Reviews***
Privacy Threshold Analyses	674
Privacy Impact Assessments	35
System of Records Notices and associated Privacy Act Exemptions	14
Privacy Act (e)(3) Statements[11]	108
Computer Matching Agreements[12]	4
Data Mining Reports	1
Privacy Compliance Reviews	2
Privacy Reviews of IT and Program Budget Requests[13]	0
Information Technology Acquisition Reviews[14] (ITAR)	200
Other Privacy Reviews	0
Total Reviews	***1,038***

[11] This total does not include all Components; several are permitted to review and approve their own Privacy Act statements by the DHS Privacy Office.
[12] CMAs are typically renewed or re-established.
[13] The Chief Information Officer 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 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, 2020, 99 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 35 PIAs: 14 new and 21 updated.

All published DHS PIAs are available on the DHS Privacy Office website, www.dhs.gov/privacy. Below is a summary of significant PIAs published during the reporting period, along with a hyperlink to the full text. A complete list of all PIAs published during the reporting period can be found in the Appendix.

New Privacy Impact Assessments

DHS/USCG/PIA-030 U.S. Coast Guard Counter-Unmanned Aircraft Systems Pilot *(October 28, 2019)*

U.S. Coast Guard (USCG) conducted an operational pilot to test and evaluate Counter-Unmanned Aircraft Systems (C-UAS) capabilities used to detect, identify, and mitigate UAS that pose a credible threat to "covered facilities or assets." USCG will continue to conduct the pilot testing through 2020, after which the USCG C-UAS program may be operationalized. This PIA discusses measures taken to mitigate privacy risks and protect against any impact to personally identifiable information during the deployment of C-UAS technologies under operational circumstances. If the USCG C-UAS program becomes fully operational, this PIA will be updated.

DHS/USSS/PIA-026 Social Media Screening *(December 6, 2019)*

United States Secret Service (USSS or Secret Service) Security Management Division procured a contract to conduct social media checks in support of the background investigation (BI) process for hiring, continuous evaluation, and periodic reinvestigation. The Secret Service uses BI processes to help mitigate the risk posed by those who potentially represent a threat to national security through proactive intervention and by identifying security-relevant information. Currently, various sources are checked for personnel security purposes, and USSS is adding a review of publicly available social media information to the existing processes that USSS security personnel use in identifying relevant information in assessing the eligibility of job applicants who have been conditionally selected for hire; reinvestigation of personnel holding clearances; and evaluation of a covered individual on an ongoing basis during the period of eligibility. The Secret Service conducted this PIA to document the collection, use, and maintenance of social media information in the BI process.

DHS/ALL/PIA-079 Department of Homeland Security (DHS) Immigration-Related Information Sharing with U.S. Census Bureau *(December 20, 2019)*

Pursuant to Executive Order (E.O.) 13880, *Collecting Information About Citizenship Status in Connection with the Decennial Census*, issued July 11, 2019, DHS provided the Department of Commerce (DOC) and the U.S. Census Bureau (Census or Census Bureau) with administrative records to assist in determining the number of citizens, lawfully present non-citizens, and unauthorized immigrants residing in the United States to fulfill the requirements of the E. O. DHS shared various data elements that the Census Bureau has articulated a need to know for the purpose of executing the E.O., including personally identifiable information, with Census to (1) update 2020 Census person files, (2) produce Citizen Voting Age Population Statistics, and (3) conduct testing of citizenship models. DHS published this PIA to describe the establishment of a formal Memorandum of Agreement between DHS and the Census Bureau, and to analyze the collection, use, and dissemination of DHS information by Census.

DHS/ALL/PIA-080 CBP and ICE DNA Collection *(January 3, 2020)*

U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE), as federal law enforcement agencies, are statutorily mandated to collect deoxyribonucleic acid (DNA) from certain individuals who come into their custody. CBP and ICE began to collect DNA from persons who are detained under the authority of the United States consistent with the *DNA Fingerprint Act of 2005*. To support this effort, the Federal Bureau of Investigations (FBI) Laboratory ("FBI Laboratory") provides Buccal Collection Kits to both CBP and ICE. CBP and ICE use these kits to collect the DNA via buccal cheek swabs and will send the DNA samples to the FBI, which in turn will process them and store the resulting DNA profile in the FBI's Combined DNA Index System (CODIS) National DNA Index System (NDIS) (CODIS/NDIS). NDIS contains DNA profiles contributed by federal and state agencies and participating forensic laboratories. CBP and ICE conducted this joint PIA to analyze the associated privacy risks with this biometric collection.

DHS/ICE/PIA-052 Visa Security Program - Pre-Adjudicated Threat Recognition Intelligence Operations Team (PATRIOT) Tracking System *(March 10, 2020)*

The Visa Security Program - Pre-Adjudicated Threat Recognition Intelligence Operations Team (PATRIOT) is an ICE tracking system designed to support the activities of the ICE Homeland Security Investigations Visa Security Program (VSP). ICE originally deployed VSP-PATRIOT in 2014, and it is operated by the Visa Security Coordination Center (VSCC), the primary national security and counterterrorism planning component for ICE, in partnership with CBP and the U.S. Department of State (DOS). VSP-PATRIOT allows authorized personnel from ICE, CBP, and DOS to identify applicants for U.S. visas who are ineligible to receive visas and inadmissible to the United States due to criminal history, terrorism-related associations or activity, other security-related offenses, or any other grounds of ineligibility or inadmissibility. ICE conducted this PIA in the interest of transparency as the VSP-PATRIOT tracking system automates the system-to-system connections memorialized in the existing Visa Security Program Tracking System-Network (VSPTS-Net) PIA.

Updated Privacy Impact Assessments

DHS/CBP/PIA-002(e) Global Enrollment System (GES): Global Entry Facial Recognition *(December 13, 2019)*

U.S. Customs and Border Protection (CBP) operates Global Entry, a program that provides dedicated processing for pre-approved travelers arriving in the United States. Program participants volunteer to provide their personally identifiable information and consent to CBP security vetting in return for expedited processing at designated U.S. Ports of Entry, or for access to sensitive CBP-controlled areas or positions. CBP updated this Privacy Impact Assessment to provide notice to the public regarding the upgrade of Global Entry kiosks with facial recognition technology to facilitate traveler identification and entry processing.

DHS/CISA/PIA-030(a) Continuous Diagnostics and Mitigation (CDM) *(December 19, 2019)*

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) 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 tools and services to strengthen the security posture of participating federal civilian departments and agencies' systems and networks. CDM establishes a suite of capabilities that enable network security officials and administrators to know the state of their respective networks at any given time, inform Chief Information Officers (CIO) and Chief Information Security Officers (CISO) on the relative risk of threats, and make it possible for government personnel to identify and mitigate vulnerabilities. This Privacy Impact Assessment (PIA) Update was conducted to assess the privacy risks related to the CDM Shared Service Platform, which makes CDM capabilities available for use by non-Chief Financial Officer (CFO) Act agencies. The Shared Service Platform is provided to non-CFO Act agencies using a third-party contractor to CISA that connects the agency's network(s) to the platform. Additionally, this PIA Update examines the CDM Agency-Wide Adaptive Risk Enumeration (AWARE) capability. The CDM AWARE capability allows participating agencies to better assess and prioritize cybersecurity risks by assigning a risk score to agency vulnerabilities.

System of Records Notices

The Department publishes System of Records Notices (SORN) consistent with the requirements outlined in the *Privacy Act of 1974, as amended*.[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 and Congress.

As of March 31, 2020, 100 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the PRIV published eight SORNs: three new, three updated, two rescindments, and six Privacy Act rulemakings.

All published DHS SORNs and Privacy Act rulemakings are available on the DHS Privacy Office website, www.dhs.gov/privacy. Below is a summary of significant SORNs published during the reporting period, along with a hyperlink to the full text in the *Federal Register*. A complete list of all SORNs published during the reporting period can be found in the Appendix.

New System of Records Notices

DHS/ALL-043 Enterprise Biometric Administrative Records

The purpose of this system of records is to collect and maintain administrative and technical records associated with the enterprise biometric system known as the Automated Biometric Identification System and its successor information technology system, currently in development, called the Homeland Advanced Recognition Technology. This system enables execution of administrative functions of the biometric repository such as redress operations, testing, training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses. *(85 Fed. Reg. 14955, March 16, 2020)*

Updated System of Records Notices

DHS/ALL-038 Insider Threat Program

The purpose of this system is to detect, deter, and mitigate insider threats. DHS uses the system to facilitate management of insider threat inquiries; identify and track potential insider threats to DHS; manage referrals of potential insider threats to and from internal and external partners; provide authorized assistance to lawful administrative, civil, counterintelligence, and criminal investigations; and generate statistical reports and meet other insider threat reporting requirements.
(85 Fed. Reg. 13914, March 10, 2020)

DHS/CBP-002 Trusted and Registered Traveler Programs

The purpose of this system is to assess on an ongoing basis applicants' eligibility for enrollment in trusted traveler and registered traveler programs. U.S. Customs and Border Protection (CBP) collects and maintains records on individuals who voluntarily provide their personally identifiable information to CBP in return for enrollment in a program that will make them eligible for dedicated CBP processing at designated U.S. border ports of entry, including all trusted traveler and registered traveler programs.

[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. *DHS Privacy Policy Instruction 047-01-004 for Privacy Compliance Reviews* implements DHS Directive 047-01, "Privacy Policy and Compliance," regarding 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.

A PCR may result in a public report or internal recommendations, depending upon the sensitivity of the program under review. The DHS Privacy Office tracks implementation of PCR recommendations based on supporting evidence provided by the Component Privacy Office and/or Program reviewed. A list of PCR recommendations that have yet to be implemented are listed on the DHS Privacy Office website, www.dhs.gov/privacy, under Privacy Oversight, along with all of the public-facing PCRs.

The DHS Privacy Office finalized two PCRs during this reporting period.

Office of the Chief Security Officer's Foreign Access Management Program
On October 3, 2019, the DHS Privacy Office finalized a classified PCR of the Chief Security Officer's Foreign Access Management Program that focused on improving the collection, protection, and sharing of data used to process requests from foreign persons seeking to visit government offices and locations. The PCR made recommendations to improve the involvement of and oversight by the Office's privacy point of contact and sought improvements in the clarification of roles, training, and the program's data handling throughout its lifecycle.

FEMA's Information Sharing Practices
On October 21, 2019, the DHS Privacy Office finalized a PCR of the Federal Emergency Management Agency (FEMA) that focused on information sharing practices and oversight. The PCR was launched in response to two major privacy incidents that occurred during Fiscal Year 2019. The DHS Privacy Office made six recommendations to improve FEMA's implementation of information sharing and safeguarding activities to better protect individuals' privacy. Due to FEMA's unique structure and the authorities granted to its regional offices, recommendation number two is particularly important to protect individuals' privacy and ensure consistency across the nation:

- *FEMA should ensure it adequately involves the FEMA Privacy Branch nationwide and in all information sharing activities to implement DHS Privacy and Information Sharing Policy.*

II. ADVICE AND RESPONSES

This section highlights privacy policy guidance and recommendations provided by the DHS Privacy Office.

Privacy Officer Recommendations

The DHS Privacy Office initiated a new process whereby additional recommendations to mitigate privacy risk are included in certain Privacy Impact Assessments. The first PIA to include "DHS Privacy Office Recommendations" is DHS/USCIS/PIA-013-01(a), Fraud Detection and National Security Directorate (Social Media), and it contains seven recommendations.

Privacy Policy Initiatives

Social Security Number Reduction Policy

The DHS Privacy Office issued a new privacy policy instruction requiring all new and legacy DHS IT systems, programs, and forms to use a unique alternative identifier to the Social Security number (SSN). If there are technological, legal, or regulatory limitations to eliminating the SSN, then privacy-enhancing SSN alternatives must be utilized, such as masking, redacting, or truncating the SSN in digital and hard copy formats.

During the reporting period:

1. The DHS Privacy Office is working with the Science and Technology Directorate to engage a vendor to develop a Decentralized Identifier or DID. This is a Globally Unique Identifier without the need for a central registration authority that is immutable over time, globally-resolvable, privacy-respecting, and cryptographically verifiable; and
2. The Office of the Chief Human Capital Officer (OCHCO) initiated a pilot of its SSN alternative, the Person Handle, in a human capital system.

Privacy Policy Assessment Project

The DHS Privacy Office is conducting an evaluation of privacy policies,[16] directives, and instructions to ensure compliance with Departmental requirements, that technical content is updated and accurate, and that policies are in line with updated legislative requirements, including citation updates. Next steps in the multi-phase evaluation include preparing updates to the first set of identified policies, directives, and instructions and reformatting legacy policies to better facilitate use and reference. Future phases will include implementing processes to conduct interval-based reviews, ascertaining whether the current policy inventory addresses DHS Privacy Office operational needs, and developing a formal communications and implementation strategy for new and existing policies. To date, six Privacy Policy Directives and Instructions have been reviewed and updated by a DHS Privacy Office cross-functional team and approved by senior leadership.

[16] DHS privacy policies available at: https://www.dhs.gov/privacy-policy-guidance.

III. TRAINING AND OUTREACH

Mandatory Online Training

119,013 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.

1,737 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 DHS Privacy Office-adjudicated Component Social Media Operational Use Template(s).

Classroom Training

2,721 DHS personnel attended instructor-led privacy training courses, including the following for which the DHS Privacy Office either sponsored or provided a trainer:

- ***FOIA Training***: This periodic training is tailored to FOIA staff throughout the Department responsible for processing FOIA requests.
    - **January 20, 2020 – Requirements for Scoping Non-Responsive Records out of a FOIA Production.** FEMA staff led a training session for DHS Privacy Office FOIA processors on determining what constitutes a record under FOIA and recent case law regarding excluding material as non-responsive.
    - **February 20, 2020 - Department of Justice FOIA Refresher Training.** Staff from the Department of Justice Office of Information Policy provided a one-day overview of FOIA's procedural requirements and the legal standards of the exemptions. DHS Privacy Office staff and Component FOIA employees attended the training, which was primarily intended for DHS FOIA employees with less than one-year experience, or FOIA employees who need a refresher course.
    - **March 12, 2020 - FOIA Training for Information Law Attorneys.** Staff from the DHS Privacy Office and the Office of General Counsel provided training to assist information law attorneys in advising clients on common FOIA issues and representing the agency's interests in FOIA litigation. Attorneys from Headquarters and the Components participated in the online training session, and a recording of the webinar was posted on DHS Connect.
    - **March 2020 - Sunshine Week FOIA Training Webinar Series.** This year's Sunshine Week FOIA Training Summit was converted into a series of virtual training sessions made available on the DHS Intranet. The DHS Privacy Office has also provided links to some of the recorded webinars and presentations to colleagues at the Department of the Treasury, Consumer Financial Protection Bureau, and the National Aeronautics and Space Administration.
- ***International Attaché Training***: The Department's International Pre-Deployment 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 DHS Privacy Office provides an international privacy policy module to raise awareness among new attachés of the potential impact global privacy policies may have on DHS operations.
- ***International Delegations***: On February 7, 2020, the DHS Privacy Office hosted a nine-member delegation from the Chilean Transparency Council. The DHS Privacy Office provided the

delegation with information on how DHS manages FOIA requests, as well as best practices and lessons learned on emerging issues in data privacy and transparency.

- ***New Employee Orientation***: The DHS 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 DHS 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 Briefings for Headquarters Staff*:** During Fiscal Year 2020, the DHS Privacy Office is providing classroom privacy awareness training to all Headquarters staff with an emphasis on identifying and solving PII data handling vulnerabilities.
- ***Role-Based Training***: In Fiscal Year 2020, the DHS Privacy Office will train all DHS Contracting Officers and Contracting Office Representatives on how to embed privacy protections into contracts. Acquisition management staff were trained first and mandated the course as required training for all Acquisition staff.
- ***DHS Privacy Office Boot Camp***: The DHS Privacy Office periodically trains new privacy staff in the Components in compliance best practices, including how to draft PTAs, PIAs, and SORNs.
- ***Reports Officer Certification Course*:** The DHS Privacy Office provides privacy training to reports officers who prepare intelligence reports as part of the DHS Intelligence Enterprise certification program.
- ***Security Specialist Course*:** The DHS Privacy Office provides privacy training every six weeks to participants of this week-long inter-agency training program.

DHS Privacy Office Outreach

DHS 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.

- **InConfidence USA Conference**: On November 14, 2019, in New York, NY, the Privacy Office presented on *Embedding Privacy into the Use of Facial Recognition at Airports.*
- **Federal Privacy Council's Annual Federal Privacy Summit**: On December 2, 2019, in Bethesda, MD, the Privacy Office moderated a panel of subject matter experts from CBP, TSA, and the Federal Trade Commission on *Embedding Privacy into the Use of Facial Recognition at Airports.*
- **Biometric Entry-Exit Meeting**: On December 3, 2019, in Washington, DC, CBP officials and the Privacy Office met with leading privacy experts to discuss CBP's implementation of the congressional biometric entry-exit mandate. The meeting was the third in an ongoing series of discussions about measures that CBP is taking to protect traveler privacy during the biometric facial comparison process at U.S. ports of entry.
- **Federal Privacy Council's Privacy Bootcamp:** On March 9, 2020, in Washington, DC, the Privacy Office conducted the first day of this eight-week course with a session entitled, *Privacy 101: Privacy at a Federal Agency*.

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.

Cybersecurity and Infrastructure Security Agency (CISA)

- Provided privacy briefings during New Employee Orientation to all new employees.
- Trained Executive Secretariat employees on how to safeguard PII when handling correspondence.
- Published two privacy-related articles in CISA's weekly newsletter, *CISA Vision,* and two issues of the quarterly privacy newsletter, *CISA Privacy Update*. The newsletter is distributed CISA-wide and posted on the CISA Office of Privacy internal intranet page.
- Participated on two panels, *Privacy Considerations in Cybersecurity Privacy* and *Security and Privacy in Smart City Initiatives*, along with representatives from government, civil liberties organizations, and academia. at the 2019 CISA Cybersecurity Summit on September 19, 2019.
- Presented on the topic of *Cybersecurity and Your Personal Information: Balancing Your Right to Information Access with Your Need for Privacy* at the Government Printing Office's 2019 Federal Depository Library Conference on October 23, 2019. The presentation gave federal depository librarians tips on cyber hygiene techniques for themselves and their patrons, and discussed cybersecurity-themed programming for their local communities.
- Participated in a panel discussion called *Think Like the Adversary*, at the 2019 Federal Privacy Summit hosted by the Federal Privacy Council on December 2, 2019.
- Spoke on a virtual panel on the topic of oversharing online to 70 public and private sector individuals as a part of CISA and the National Cyber Security Agency (NCSA) for the STOP. THINK. CONNECT.™ January 2020 Partner Call in recognition of Data Privacy Day.
- Served as a keynote speaker on the topic of *Privacy: Data Security is National Security* at the 2020 U.S. Census Bureau Privacy Day, discussing CISA's "National Critical Functions" and how the protection of sensitive information fits into the functions and daily activities of Census employees.

Federal Emergency Management Agency (FEMA)

- Hosted a Stand-Down Initiative agency-wide in February 2020 with over 3900 attendees to provide each region with training and tools to self-report all information sharing.
- Collaborated with the Chief Contracting Office to develop training materials that were presented live via 15 Adobe Connect/teleconference sessions over five days. These sessions were also recorded, closed-captioned, and posted on the FEMA Privacy SharePoint site for the benefit of the entire FEMA community. Participants were also invited to ask privacy-related and information sharing-related questions via Adobe Connect chat during the stand down assessment and via email; FEMA Privacy responded within 24 hours.

Science & Technology Directorate (S&T)

- Continued to engage with OGC in drafting updated social media policy guidance to cover S&T research, development, test, and evaluation efforts along with creating specific social media training to provide to S&T employees.
- DHS personnel completed instructor-led privacy training and awareness briefings and meetings with the following S&T Offices and Programs:
    - Office of National Laboratories All-Hands Meeting
    - Transportation Security Laboratory
    - Silicon Valley Innovation Program
    - Federally Funded Research & Development Centers Program Management Office

- Contract Acquisition Program Support, S&T Acquisition Quarterly

Transportation Security Administration (TSA)

- Trained ISSOs on how to draft a Privacy Threshold Analysis at ISSO Townhalls.
- Discussed biometrics at Federal Privacy Council meetings.

U.S. Citizenship and Immigration Services (USCIS)

- Provided bi-weekly privacy awareness training to onboarding USCIS Headquarters employees.
- Conducted instructor-led privacy training and awareness sessions to USCIS offices and programs, including: Office of Human Capital and Training, Office of Security and Integrity, Office of Policy and Strategy, Service Center Operations, and Field Operation offices. Trainings were provided upon request from the offices and in response to internal outreach initiatives.
- Delivered quarterly role-based in-person privacy training to operations and mission support staff. Training encompassed role-based exercises and scenarios that are centered around privacy requirements relating to administrative and human resources duties.
- Implemented the updated, required privacy training for Fraud Detection and National Security (FDNS) Directorate officers authorized to conduct social media research, to include the privacy framework for use of fictitious accounts and/or identities as a tactic within social media research. The updated training ensures compliance with the PIA on USCIS' use of fictitious accounts and/or identities for the Operational Use of Social Media.
- Trained USCIS Contracting Officer Representatives (COR) on privacy risks associated with outsourcing PII. The training placed emphasis on the HSAM Appendix G, required privacy and security safeguards, required clauses, and approval steps. Promoted privacy awareness among employees via several communication forms: quarterly email reminders on privacy policies, posters and digital signage on TV monitors displaying best practices and tips. Highlights include:
  - Five USCIS Service Centers (SCOPS) ordered 90 printed privacy posters (addressing different privacy requirements) designed and developed by the Office of Privacy to be posted in high traffic areas within office spaces. The posters will reach an estimated audience of 8,000 federal employees and contractors.
  - Designed privacy awareness information tailored to certain holidays and other significant events, including Halloween, New Year's Day, and Data Privacy Day.
  - Broadcasted an agency-wide message on employees' responsibility to properly handle sensitive information. The Office of Privacy collaborated with the Office of Information Technology to emphasize information management requirements, the authorized uses of collaboration tools during the pandemic, and the reporting of unauthorized disclosure of information.
- Developed and launched an agency-wide quiz *Privacy Matters – Test Your Knowledge*, in observation of Data Privacy Day 2020. The quiz measured employees' awareness of USCIS privacy policies.
- Redesigned the Office of Privacy intranet site. The new streamlined menus and navigation offer a user-friendly experience for USCIS personnel to locate privacy-related resources and to engage with different services on privacy matters.
- Briefed the National Vetting Center (NVC) Privacy and Civil Liberties Working Group on the Affirmative Asylum privacy risk analysis. The audience comprised privacy and CRCL personnel across DHS, and NVC Vetting Support Agencies in Virginia.

U.S. Coast Guard (USCG)

- Continued privacy presentations at the biweekly USCG Civilian Employee Orientation session. USCG Privacy focused on raising awareness of the importance of protecting personal information while assigned to DHS. In addition, USCG Privacy provided and discussed policy outlined in the DHS factsheet titled *How to Safeguard Sensitive PII (SPII)*.
- Attended an All-Hands briefing at the Coast Guard Base Portsmouth, Virginia, following a recent privacy incident, and trained over 200 personnel on proper handling of SPII reiterating personnel responsibility, and highlighted several aspects of the DHS Factsheet (How to Safeguard SPII).
- Disseminated a flyer emphasizing the requirements and instructions for encrypting or password-protecting electronic sensitive information at Coast Guard Base Portsmouth All-Hands. This flyer is also provided to Commands who are remediating incidents involving unauthorized release of un-encrypted or non-password protected PII/SPII.
- Promoted privacy awareness by posting periodic "privacy tips" on the Coast Guard Portal Special Notices page and information screens located at building entrances, cafeteria, and lunch room. One campaign highlighted privacy risk during tax season, especially scams targeting PII.

U.S. Customs and Border Protection (CBP)

- Provided privacy training during New Employee Orientations.
- Supported the Office of Field Operations during outreach efforts related to the use of facial recognition technology.
- Published privacy notices and reminders that were distributed to the workforce via the agencies Information Display System.

U.S. Immigration and Customs Enforcement (ICE)

- Provided biweekly privacy training during New Employee Orientations for 201 ICE personnel.
- Trained ICE personnel involved in Congressional Disclosures on the proper precautionary steps they must take before disclosure. This training focused on identifying potential improper disclosures before they become an issue.
- Developed and provided privacy training tailored to fit the varied needs of ICE's program offices. This includes training for mission support staff, Information System Security Officers, Enforcement and Removal Operations employees, and National Security Investigations Division employees.
- Created and disseminated implementation guidance and trainings related to DHS Privacy Policy 2017-01.

U.S. Secret Service (USSS)

- Led the USSS Breach Response Team in drafting agency directives that set guidelines for the USSS in providing efficient and effective responses to victims in the event of a major privacy breach.
- Created a USSS Policy Manual section for privacy incident response, detailing roles and responsibilities for all staff and offices.
- Promoted a privacy awareness ad campaign with posters and electronic kiosks throughout the USSS Headquarters building to help staff better differentiate PII from Sensitive PII (SPII).
- Distributed two quarterly Secret Service-wide e-mail messages to all USSS staff emphasizing responsibilities for user awareness of SPII on shared media, and another for safeguarding privacy while working remotely.

- Prepared presentation materials for and hosted an inaugural "International Privacy Day" event which included electronic kiosks and printed flyers throughout the USSS Headquarters building, a banner on the USSS Intranet home page, and a mass voicemail to all HQ employees. Activities included participatory games and presentations educating attendees on the importance of accuracy for PII data; how a few pieces of otherwise innocuous PII can be strung together to uniquely identify someone; and distinguishing phrases/terms as either PII or sensitive PII (SPII).
- Provided a focused, specialized presentation to 30 staff members involved in the auditing response process regarding proper PII safeguards and tools to use when returning responses to auditors.
- Attended a presentation by the DHS Privacy Office to the USSS Procurement Office's contracting officers on how to embed privacy into the acquisition process.

IV. PRIVACY COMPLAINTS

The DHS Privacy Office is responsible for ensuring that the Department has procedures in place to receive, investigate, respond to, and, when appropriate, provide redress for privacy complaints. As required by Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, as amended, the DHS Privacy Office is required to provide semi-annual reports to Congress with the number and nature of the complaints received by the Department for alleged violations, and a summary of the disposition of such complaints, when available.

The DHS Privacy Office reviews and responds to privacy complaints referred by employees throughout the Department, or complaints submitted by other government agencies, the private sector, or the public. DHS Components manage and customize their privacy complaint handling processes to align with their specific missions, and to comply with Department complaint handling and reporting requirements.

DHS separates privacy complaints into four types:

1. ***Procedure:*** Issues concerning process and procedure, such as consent, collection, and appropriate notice at the time of collection, or notices provided in the *Federal Register*, such as Privacy Act SORNs.
    a. *Example*: An individual alleges that a program violates privacy by collecting Social Security numbers without providing proper notice.
2. ***Redress:*** Issues concerning appropriate access (not to include FOIA or Privacy Act requests) or correction to PII held by DHS. Also includes DHS Traveler Redress Inquiry Program (DHS TRIP) privacy-related complaints. See below for more information.
    a. Example: Misidentification during a credentialing process or during traveler inspection at the border or screening at airports.
3. ***Operational:*** Issues related to general privacy concerns or other concerns that are not addressed in process or redress, but do not pertain to Privacy Act matters.
    a. *Example:* An employee's health information was disclosed to a non-supervisor.
    b. *Example:* Physical screening and pat down procedures at airports.
4. ***Referred*:** Complaints referred to another federal agency or external entity for handling.
    a. *Example:* An individual submits an inquiry regarding his driver's license or Social Security number.

In addition, the DHS Privacy Office reviews redress complaints received by the DHS Traveler Redress Inquiry Program (DHS TRIP) that may have a privacy nexus. DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs - like airports - or crossing U.S. borders. This includes watch list issues, screening problems at ports of entry, and situations where travelers believe they have been unfairly or incorrectly delayed, denied boarding, or identified for additional screening at our nation's transportation hubs.

The DHS TRIP complaint form includes a privacy check box that reads: *I believe my privacy has been violated because a government agent has exposed or inappropriately shared my personal information.* During the reporting period, there were **564** travelers who marked that box. Of those, none fit the complaint criteria listed above. *However*:

- eight complaints had a general privacy nexus regarding CBP Officers taking photos and scanning wallet contents or there was a data integrity and accuracy concern. CBP Privacy reviewed each and reported that there were no privacy act violations.
- one complaint was sent to CBP regarding alleged officer conduct. Investigation of that complaint revealed that it was an ICE Officer and not a CBP Officer involved. ICE explained the process and indicated that the traveler is under full legal investigation and no money was stolen from him.

During the reporting period, the Department received **483** privacy complaints.

Privacy Complaints Received by DHS Components and the DHS Traveler Redress Inquiry Program *October 1, 2019 – March 31, 2020*										
Type	**CBP**	**CISA**	**FEMA**	**ICE**	**TSA**	**USCG**	**USCIS**	**USSS**	**TRIP**	**TOTAL**
Procedure	5	0	0	0	1	0	0	0	0	**6**
Redress	351	0	0	0	0	0	0	0	0	**351**
Operational	13	0	0	0	113	0	0	0	0	**126**
Referred	0	0	0	0	0	0	0	0	0	**0**
TOTALS	**369**	**0**	**0**	**0**	**114**	**0**	**0**	**0**	**0**	**483**

***Narrative examples*:**

CBP

- **Redress:** Complainant, a Global Entry member for over 10 years, wrote to ask why he often has to undergo a secondary screening. CBP provided guidance to the complainant on how to correct his records to remove the flag from DHS systems.

TSA

- **Procedural**: An employee complained that an Office of Human Capital form used for scoring work performance required a full SSN without providing a Privacy Act statement explaining the consequences for failure to provide the SSN. TSA Privacy referred the complaint to Office of Human Capital officials to include a Privacy Act statement within the system that houses the form.

- **Operational**: An airline passenger complained that locks were cut off of her luggage by TSA to conduct a checked bag search. TSA Privacy provided information on TSA mission authorities related to locked luggage as well as a link to the TSA website with further information.

APPENDIX – PUBLISHED PIAS AND SORNS

Privacy Impact Assessments Published October 1, 2019 – March 31, 2020	
DHS Component and System Name	**Date Published**
ALL/PIA-007(a) DHS Correspondence and Inquiries Tracking Tools	10/31/2019
ALL/PIA-044(b) DHS Request for Information Management Tool: CBP Module	11/25/2019
ALL/PIA-076 Data Management Hub	12/26/2019
ALL/PIA-078 Geospatial Information Infrastructure	1/5/2020
ALL/PIA-079 DHS Citizenship-Related Information Sharing with U.S. Census Bureau	1/31/2020
ALL/PIA-080 DNA Collection	2/13/2020
ALL/PIA-081 Management Cube	10/22/2019
ALL/PIA-082 Continuous Monitoring as a Service	10/29/2019
CBP/PIA-001(h) Advanced Passenger Information System	1/28/2020
CBP/PIA-002(e) Global Enrollment System (GES): Global Entry Facial Recognition	12/13/2019
CBP/PIA-024(c) Arrival Departure Information System	3/9/2020
CBP/PIA-041(a) Enterprise Geospatial Information Services	2/28/2020
CBP/PIA-060 e-Allegations Portal	2/28/2020
CBP/PIA-061 Air Cargo Advance Screening	10/29/2019
CBP/PIA-062 Trusted Worker Program	12/26/2019
CISA/PIA-006(a) Protected Critical Infrastructure Information Management System (PCIIMS) Final Operating Capability (FOC)	11/13/2019
CISA/PIA-018(d) Chemical Facility Anti-Terrorism Standards Personnel Surety Program	10/30/2019
CISA/PIA-030(a) Continuous Diagnostics & Mitigation	12/15/2019
CISA/PIA-034 Protected Critical Infrastructure Program	1/13/2020
ICE/PIA-001 Student and Exchange Visitor Program	1/5/2020
ICE/PIA-052 Visa Security Program - Pre-Adjudicated Threat Recognition Intelligence Operations Team	2/27/2020
OBIM/PIA-004 Homeland Advanced Recognition Technology	12/12/2019
S&T/PIA-032(a) Science & Technology Analytical Tracking System	3/10/2020
S&T/PIA-039 Genomic Data Network and Analysis (GDNA) System	12/19/2019
USCG/PIA-030 Counter-Unmanned Aircraft System	2/20/2020
USCG/PIA-028 Defense Sexual Assault Incident Database	12/19/2019
USCIS/PIA-008(b) Enterprise Service Bus 2	12/20/2019
USCIS/PIA-016(c) Computer Linked Application Information Management System 3 Local Area Network	2/21/2020
USCIS/PIA-030(h) E-Verify Program	3/13/2020
USCIS/PIA-031(b) Citizenship and Immigration Data Repository	1/30/2020
USCIS/PIA-034(b) H-1B Cap Registration	10/30/2019
USCIS/PIA-056(b) Electronic Immigration System	3/3/2020
USSS/PIA-012(c) Electronic Name Check System	3/16/2020

Privacy Impact Assessments Published October 1, 2019 – March 31, 2020	
DHS Component and System Name	**Date Published**
USSS/PIA-016(b) Enterprise Person	10/29/2019
USSS/PIA-023(a) Applicant Lifecycle Information System	12/19/2019
USSS/PIA-026 Social Media Screening	12/26/2019

System of Records Notices Published October 1, 2019 – March 31, 2020	
DHS Component and System Name	**Date Published**
ALL-038 Insider Threat Program	3/10/2020
ALL-043 Enterprise Biometric Administrative Records	3/16/2020
ALL-045 Statistical Data Production and Reporting System	3/11/2020
CBP-002 Global Enrollment Programs	3/10/2020
CBP-017 Analytical Framework for Intelligence	3/10/2020
CBP-026 Explorer Program System	3/10/2020
USCIS-002 BCS and DHS/USCIS-003 BSS SORN Rescindment	3/11/2020
USCIS-007 Benefit Information System	10/9/2019