Privacy Office

Fiscal Year 2020 Semiannual Report to Congress

Covering the period April 1, 2020 – September 30, 2020

February 8, 2021

Homeland Security

FOREWORD

February 8, 2021

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 April 1 – September 30, 2020.[1]

Highlights
During the reporting period, the Privacy Office:

- Completed 1,592 privacy reviews, including:
  - 1,003 Privacy Threshold Analyses;
  - 45 Privacy Impact Assessments; and
  - 3 System of Records Notices and associated Privacy Act exemptions.
- Published the following congressional reports:
  - *2019 Annual Data Mining Report to Congress*
  - *2020 Social Security Number Fraud Prevention Act Report*

About the Privacy Office
The *Homeland Security Act of 2002* charges the Chief Privacy Officer (CPO) with primary responsibility for ensuring that privacy protections are integrated into all DHS programs, policies, and procedures. The CPO 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 Privacy Office centralizes DHS Headquarters FOIA and Privacy Act access and amendment operations, and provides compliance, policy, and programmatic oversight on FOIA and privacy issues across the Department. The Privacy Office undertakes these statutory and policy-based responsibilities in collaboration with 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.

Sincerely,

James V.M.L. Holzer
Chief Privacy Officer and Chief FOIA Officer, Acting
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 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.

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

The Honorable Kamala Harris
President, U.S. Senate

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

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

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

The Honorable Dick Durbin
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Chuck Grassley
Ranking Member, U.S. Senate Committee on the Judiciary

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

The Honorable Marco Rubio
Ranking Member, U.S. Senate Select Committee on Intelligence

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

The Honorable John Katko
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Carolyn Maloney
Chairwoman, 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

Privacy Office
Fiscal Year 2020
Semiannual Report to Congress

Table of Contents

I. PRIVACY REVIEWS

The 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 CPO 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 CPO.

[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 CPO and 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 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 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 1: Privacy Reviews Completed ***April 1- September 30, 2020***	
Type of Review	***Number of Reviews***
Privacy Threshold Analyses	1,003
Privacy Impact Assessments	45
System of Records Notices and associated Privacy Act Exemptions	3
Privacy Act (e)(3) Statements[11]	101
Computer Matching Agreements[12]	7
Data Mining Reports	1
Privacy Compliance Reviews	0
Privacy Reviews of IT and Program Budget Requests[13]	46
Information Technology Acquisition Reviews	386
Other Privacy Reviews	0
Total Reviews	***1,592***

[11] This total does not include all Components; several are permitted to review and approve their own Privacy Act statements by the 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.

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 September 30, 2020, 98 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 45 PIAs: 23 new and 22 updated.

All published DHS PIAs are available on the 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/ICE/PIA-054 ICE Use of Facial Recognition Services *(May 13, 2020)*
Homeland Security Investigations (HSI) is the investigative arm of U.S. Immigration and Customs Enforcement (ICE), focused on countering domestic and transnational crimes. In the course of its investigations, HSI routinely encounters digital images of potential victims or individuals suspected of crimes, but cannot connect those images to identifiable information through existing investigative methods. Therefore, HSI submits those images to government agencies and commercial vendors to compare against their digital image galleries via facial recognition processes. The agencies and vendors query their databases for potential matches, and return lists of potential candidate matches that HSI can use to produce investigative leads. HSI conducted this PIA because the use of these facial recognition services requires the collection, maintenance, and use of PII.

DHS/ALL/PIA-085 Counter-Unmanned Aircraft Systems (C-UAS) (*July 15, 2020)*
DHS is leading efforts and coordinating across the Federal Government on testing and evaluating technologies used to detect, identify, monitor, and, if needed, mitigate unmanned aircraft systems (UAS) that pose a credible threat to covered facilities, assets, and other missions authorized by law. These protective technologies are referred to as C-UAS. This PIA discusses measures taken to mitigate privacy risks and protect PII during DHS's use of C-UAS technologies during testing, evaluation, and operational deployment.

DHS/ALL/PIA-080 CBP and ICE DNA Collection *(July 23, 2020)*
DHS, U. S. Customs and Border Protection (CBP), and 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 swab, and then send the DNA samples to the FBI, which in turn process them and stores 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 provide notice to the public regarding this biometric collection and to analyze the associated privacy risks. DHS is reissuing this PIA, originally published on January 3, 2020, to note that the CBP Office of Field Operations is expanding the minimum age for DNA collection from 18 to 14.

DHS/CWMD/PIA-001 Medical and Public Health Information Sharing Environment (MPHISE) *(July 24, 2020)*
The DHS Countering Weapons of Mass Destruction Office (CWMD) maintains the MPHISE system. MPHISE is designed to provide a secure networking capability between DHS personnel and designated federal, state, local, territorial, tribal, and private sector medical and public health partners. This PIA supports MPHISE to be used as a platform to enable information sharing across the extended medical and public health community in response to any chemical, biological, radiologic, and/or nuclear threat. Standard sharing includes anonymized health information, but in some cases, non-anonymized health data and Sensitive PII will be shared.

DHS/ALL/PIA-086 DHS Counterintelligence Program *(August 31, 2020)*
The DHS Counterintelligence (CI) Program is a Department-wide effort designed to detect, deter, and disrupt foreign intelligence threats directed at the United States. CI encompasses those activities that identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents (including transnational criminal organizations and drug trafficking organizations conducting intelligence-related activities), or international terrorist organizations or activities. DHS conducted this PIA because the DHS CI Program requires access to, collection of, and storage of PII associated with individuals who are either involved in, witness to, or knowledgeable of CI-related activities that are the subject of inquiry by DHS, or supporting CI activities conducted by the DHS CI Program.

Updated Privacy Impact Assessments

DHS/TSA/PIA-046(b) Travel Document Checker Automation Using Facial Recognition *(June 3, 2020)*
The Transportation Security Administration (TSA) enhances the identity verification of passengers by using facial verification technology at airports. In a previous proof of concept, TSA used a Credential Authentication Technology (CAT) device equipped with a camera (CAT-C) to validate that the identity document presented by the passenger was authentic, and to compare the passenger's live facial image against the image from the passenger's identity document. Building on its previous work, TSA now networks the CAT-C to the TSA Secure Flight system so that passenger boarding pass information can be passed from Secure Flight to the CAT-C. This provides improved real-time boarding pass instructions with improved identity matching and reduced physical handling of travel documents to limit unnecessary exposure, such as during the Coronavirus (COVID-19) pandemic. This PIA was conducted pursuant to Section 222 of the Homeland Security Act to address privacy risks in the use of technology in connecting the CAT-C to the TSA Secure Flight system, displaying Secure Flight data on the CAT-C, and integrating Secure Flight data in the identity verification process.

DHS/ALL/PIA-043(a) Office of the Chief Human Capital Officer (OCHCO) Talent Acquisition *(September 11, 2020)*
Talent Acquisition is a federal human capital business function whereby federal agencies establish internal programs and procedures for attracting, recruiting, assessing, and selecting employees with the right skills and competencies in accordance with federal merit system principles. Talent Acquisition includes aligning workforce plans to organizational strategies and business needs, recruiting qualified individuals, evaluating candidates, processing suitability determinations, and integrating new employees into the Department. OCHCO and Component Human Capital Offices rely on various systems to support Talent Acquisition processes. DHS conducted this PIA, which updates and replaces the previous DHS Hiring and On-Boarding PIA, because the systems that support Talent Acquisition collect, use, store, and transmit Sensitive PII.

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*.[14] 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 September 30, 2020, 100 percent of the Department's FISMA systems that require a SORN had an applicable SORN. During the reporting period, the Privacy Office published two SORNs: one new, one updated, 0 rescindments, and one Privacy Act rulemakings.

All published DHS SORNs and Privacy Act rulemakings are available on the 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-047 Records Related to DHS Personnel, Long-Term Trainees, Contractors, and Visitors During a Declared Public Health Emergency
The purpose of this system is to maintain records to protect the Department's workforce and respond to a declared public health emergency. For instance, DHS may use the information collected to conduct contact tracing. *(85 Fed. Reg. 45914, July 30, 2020)*

Updated System of Records Notices

DHS/U.S. Citizenship and Immigration Services (USCIS)-004 Systematic Alien Verification for Entitlements (SAVE) Program
The purpose of this system is to provide a fee-based service that assists federal, state, tribal, and local government agencies, benefit-granting agencies, private entities, institutions, and licensing bureaus for any legally mandated purpose in accordance with an authorizing statute to confirm immigration and

[14] 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.

naturalized and certain derived citizen status information, and to otherwise efficiently administer their programs, to the extent that such disclosure is necessary to enable these agencies and entities to make decisions related to (1) determining eligibility for a federal, state, tribal, or local public benefit; (2) issuing a license or grant; (3) issuing a government credential; (4) conducting a background investigation; or (5) any other lawful purpose. This system is also used for USCIS bond management purposes under sec. 213 of the *Immigration and Nationality Act*. *(85 Fed. Reg. 31798, May 27, 2020)*

Privacy Compliance Reviews

The 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 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 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 Privacy Office website, www.dhs.gov/privacy, under Privacy Oversight, along with all of the public-facing PCRs.

- No PCRs were published during this reporting period.

II. ADVICE AND RESPONSES

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

Privacy Policy Initiatives

Social Security Number Reduction Policy

The 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 Privacy Office, in collaboration with the Science and Technology Directorate, engaged 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 Privacy Office is conducting an evaluation of privacy policies,[15] 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 Privacy Office operational needs, and developing a formal communications and implementation strategy for new and existing policies.

2020 Virtual Privacy Incident Tabletop Exercise

In September 2020, the Privacy Office hosted, in conjunction with the Federal Emergency Management Agency's (FEMA) National Exercise Division, the third Annual DHS Privacy Incident Tabletop Exercise. This virtual event was attended by over 140 Department personnel to validate and test the DHS breach response plan. In addition, this year's exercise included a presentation on the Homeland Security Acquisitions Regulation contract clauses for "Safeguarding of Sensitive Information," a discussion on lessons learned from major privacy incidents at DHS, as well as a discussion on contract vehicles for notification and credit monitoring services.

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

III. Training and Outreach

Training

Mandatory Online Training

164,075 DHS personnel completed the mandatory computer-assisted privacy awareness training course, Privacy at DHS: Protecting Personal Information. This course is required for all personnel when they join the Department, and annually thereafter.

4,764 DHS personnel completed Operational Use of Social Media Training during this reporting period, as required by DHS Directive Instruction Number 110-01-001, Privacy Policy for Operational Use of Social Media, and applicable Privacy Office-adjudicated Component Social Media Operational Use Template(s).

Classroom Training

5,115 DHS personnel attended instructor-led privacy training courses, including the following that the Privacy Office either sponsored or provided a trainer:

- ***FOIA Training***: The Privacy Office provided FOIA training to employees during new employee orientation, and continued to record and make available training sessions online using recording through Adobe Connect. Links to the recordings were sent to all FOIA employees within the Department, and at the Department of the Treasury, National Aeronautics and Space Administration (NASA), and the Consumer Financial Protection Board (CFPB).
    - The Privacy Office also provided the following training (with estimated attendees):
        - FOIA overview: 6 attendees
        - Video redaction demonstration: 15 attendees
        - Significant FOIA requests and Consultations: 50 attendees
- ***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 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.
    - Due to the pandemic, no classes were held this period.
- ***New Employee Orientation***: 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.
    - 577 new employees were trained this period.
- ***Privacy Briefings for Headquarters Staff***: During Fiscal Year 2020, the Privacy Office provided classroom or virtual privacy awareness training to many Offices within DHS Headquarters staff, with an emphasis on identifying and solving PII data handling vulnerabilities.
- ***Role-Based Training***: In Fiscal Year 2020, the Privacy Office trained all management staff in the Procurement Office on how to embed privacy protections into contracts.
- ***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.

- ***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.
    - 38 Reports Officers were trained this period.
- ***Security Specialist Course***: The Privacy Office provides privacy training every six weeks to participants of this week-long inter-agency training program.
    - Due to the pandemic, no classes were held this period.
- ***Fusion Center Training***: The Privacy Office provides periodic training to Privacy Officers in the fusion centers across the country.
    - During this period, 10 fusion center privacy, civil rights, and civil liberties officers from across the country received training as part of a pilot program with the Office for Civil Rights and Civil Liberties (CRCL), focused on developing and implementing privacy policies, effective oversight and governance mechanisms, and responding to data breaches.

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.

- **Federal Privacy Council's Virtual Privacy Bootcamp**: On July 17, 2020, the Senior Director for Privacy Policy and Oversight presented a class on *Web Policies* as part of an eight-week course designed to train new privacy professionals in the Federal Government on privacy fundamentals and best practices.

- **American Society of Access Professionals (ASAP) Virtual National Training Conference**: Held on July 28 - 29, 2020, provided concentrated in-depth FOIA training to more than 300 individuals. A Privacy Office employee chaired the Conference Committee, and DHS FOIA professionals, including representatives from the Privacy Office, CBP, USCIS and FEMA led many of the sessions.

- **Federal Privacy Council's Virtual Annual Federal Privacy Summit**: The Privacy Office worked with the Office of Management and Budget to plan the first virtual Summit, drawing over 500 privacy professionals from across the Federal Government on October 16, 2020. The Acting Senior Director for Privacy Compliance participated in a panel discussion on *Privacy and the Pandemic.*

Component Privacy Office Training and Outreach

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

Cybersecurity and Infrastructure Security Agency (CISA)

- Trained 44 individuals across CISA regarding the privacy review in the Information Technology Acquisition Review process.
- Provided a Privacy briefing during New Employee Orientation to a total of 206 new CISA employees across all divisions.
- Produced two issues (June and September 2020) of the quarterly privacy newsletter, *CISA Privacy Update*. The newsletter is distributed CISA-wide and posted on the CISA Office of the CPO Intranet site.

Science & Technology Directorate (S&T)

- Continued to engage with the Office of the General Counsel in drafting updated social media policy guidance to cover S&T research, development, testing, and evaluation efforts along with creating specific social media training and rules of behavior to provide to S&T employees.
- Refreshed the introductory Privacy 101 training content provided to all new S&T employees and contractors during orientation.
- Participated in a panel discussion with Office of the Chief Information Officer and Chief Security Officer to explain the Homeland Security Acquisition Manual (HSAM) Appendix G review process and its implications for compliance responsibilities to S&T Program Managers and staff.
- DHS personnel completed instructor-led privacy training and awareness briefings, and meetings with the following S&T Offices and Programs:
    - DHS Federally Funded Research and Development Centers
    - Homeland Security Systems Engineering Development Institute
    - Homeland Security Operational Analysis Center
    - Office of Mission and Capability Support
    - Office of Science and Engineering Technology Centers Division
    - Office of University Programs Centers of Excellence
    - Program Managers User Group
    - Integrated Multi-Domain Enterprise
    - Executive Directors and Principal Directors Roundtable

Transportation Security Administration (TSA)

- Conducted outreach activities with over 317 TSA personnel and members of the public during the reporting period, including training on civil liberties issues for Intelligence Reporting, and outreach on TSA facial identity verification technology.

U.S. Citizenship and Immigration Services (USCIS)

- Provided bi-weekly privacy awareness training to onboarding USCIS Headquarters employees.
- Conducted instructor-led virtual privacy training and awareness sessions to USCIS offices and programs.
  Trained Fraud Detection and National Security (FDNS) Directorate officers authorized to conduct social media research using fictitious accounts and/or identities. The new training ensures compliance with the PIA on USCIS' use of fictitious accounts and/or identities for the Operational Use of Social Media

U.S. Coast Guard (USCG)

- Trained all new employees on the importance of protecting personal information at the biweekly USCG Civilian Employee Orientation sessions.

U.S. Customs and Border Protection (CBP)

- Provided virtual training to over 331 individuals through several Program Offices to include: Office of International Affairs, Office of Intelligence, Human Resources Management, Office of Trade, and several Trusted Traveler Program offices. The trainings ranged from foundational refresher privacy training (including some 'Train the Trainer' sessions), privacy compliance training, information sharing training (which also included Delegated Authority trainings), and operational use of social media privacy training.
- Broadcast seasonal messages on the Information Display System to heighten awareness of employees' responsibilities to safeguard PII.
- Hosted a 'brown bag lunch series' training with the Office of Acquisitions to facilitate discussions of privacy inclusion in contract administration with respect to the Homeland Security Acquisition Review clauses and other privacy fundamentals.

U.S. Immigration and Customs Enforcement (ICE)

- Trained approximately 280 ICE personnel in 13 virtual New-Hire Orientation privacy training sessions.
- Trained 60 ICE Mission Support personnel. Training covered records management, FOIA obligations, and other data management concepts.
- Trained 14 DHS and components on privacy breach incident handling during DHS incident handling "Tabletop" exercises.
- Provided the following online training courses:
    - 20,517 ICE personnel have completed the online course Privacy at DHS: Protecting Personal Information.
    - 39 ICE personnel have completed operational use of social media training during the reporting period, as required by DHS Directive Instruction Number 110-01-001, Privacy Policy for Operational Use of Social Media.
    - 9,878 ICE personnel have completed the following online modules:
        - Cybersecurity Awareness Training (CSAT) (9,667 users);
        - Privacy Training for SharePoint Collaboration Site Users (197 users);
        - ICE Social Engineering Training (ISET) for All Users (Computer Based; 14 users)
- Trained Office of Congressional Relations staff and leadership in other ICE offices in proper disclosure procedures to prevent the improper release of sensitive information.
- Provided procurement training to Office of the Chief Information Officer and Office of Acquisition Management, focusing on the intersection of privacy and procurements.
- Provided role-based training for Enforcement and Removal Operations, Homeland Security Investigations, and Student and Exchange Visitor Program personnel.

U.S. Secret Service (USSS)

- Trained nine new Inspectors and Assistant Inspectors on privacy requirements and criteria to be reported as they conduct internal office audits in headquarters and field offices throughout the agency.

IV. PRIVACY COMPLAINTS

The 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. The 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.
    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 without a need to know.
    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 Privacy Office reviews redress complaints received by 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 period April 1 – September 30, 2020, there were 231 travelers who marked that box. Of the 231 complaints, none fit the criteria above. Due to COVID-19 travel restrictions, the Department saw a significant drop in complaints starting in April 2020.

During the reporting period, the Department received **70** privacy complaints.

Table 2: Privacy Complaints Received by DHS Components and the DHS Traveler Redress Inquiry Program
April 1– September 30, 2020

Type	CBP	CISA	FEMA	ICE	TSA	USCG	USCIS	USSS	TRIP	TOTAL
Procedure	3	0	0	0	0	0	0	0	0	**3**
Redress	0	0	0	0	0	0	0	0	0	**0**
Operational	33	0	0	3	31	0	0	0	0	**67**
Referred	0	0	0	0	0	0	0	0	0	**0**
TOTALS	**36**	**0**	**0**	**3**	**31**	**0**	**0**	**0**	**0**	**70**

***Narrative examples*:**

TSA
Operational:

- An individual complained that a former TSA employee currently employed by a municipal police department used the complainant's identity to launder money and sexually assaulted her. TSA Privacy recommended the individual contact local law enforcement.
- A passenger complained that her checked bag was searched by TSA. TSA Privacy provided information on TSA search authorities.

ICE
Operational:

- Two ICE employees reported that their health information was disclosed without their authorization and was used beyond the intended purposes by their supervisors. ICE Privacy reviewed the cases and determined that these incidents required further investigation and intervention by the ICE Office of Professional Responsibility (OPR).
- An ICE employee reported that a supervisor disclosed his performance work plan to an unauthorized individual who did not have a valid need-to-know. ICE Privacy reviewed the case and determined that the incident required further investigation and intervention by ICE OPR.

Note: Due to other pending investigations related to the cases mentioned above, ICE Privacy conducted the preliminary review and gathering of information (to the extent permissible) and referred the complaints to ICE OPR for further investigation.

APPENDIX – PUBLISHED PIAS AND SORNS

Privacy Impact Assessments Published April 1– September 30, 2020	
DHS Component and System Name	**Date Published**
DHS/ALL/PIA-083 Targeted Violence and Terrorism Prevention	4/8/2020
DHS/USSS/PIA-027 Targeted School Violence Database	4/9/2020
DHS/USCG/PIA-005(a) Maritime Analytic Support System	4/23/2020
DHS/ALL/PIA-084 Joint Threat Information Management System	4/24/2020
DHS/TSA/PIA-020(c) Security Threat Assessment for Airport Badge and Credential Holders	4/24/2020
DHS/USCIS/PIA-068(a) Refugee Case Processing and Security Vetting	4/24/2020
DHS/CBP/PIA-057(a) Electronic Secured Adjudication Forms Environment	4/26/2020
DHS/CBP/PIA-063 Enterprise Analytics	5/5/2020
DHS/ICE/PIA-053 Training Management Support System (TMSS)	5/5/2020
DHS/USSS/PIA-017(a) Forensic Services Division Suite	5/8/2020
DHS/ICE/PIA-054 ICE Use of Facial Recognition Services	5/12/2020
DHS/ICE/PIA-055 Repository for Analytics in a Virtualized Environment	5/12/2020
DHS/USSS/PIA-028 Unmanned Aircraft System	5/22/2020
DHS/CBP/PIA-029(a) REMEDY Enterprise Services Management System	5/26/2020
DHS/FEMA/PIA-055 FEMA Response Use of Unmanned Aircraft System (UAS) Derived Imagery	5/27/2020
DHS/ICE/PIA-056 War Crime Hunter	5/28/2020
DHS/TSA/PIA-046(b) Travel Document Checker Automation Using Facial Recognition	6/3/2020
DHS/FEMA/PIA-051(a) Physical Access Control System	6/22/2020
DHS/USCIS/PIA-016(d) Computer Linked Application Information Management System and Associated Systems	6/30/2020
DHS/USCIS/PIA-056(c) Electronic Immigration System	6/30/2020
DHS/USCIS/PIA-006(c) Systematic Alien Verification for Entitlements Program	7/1/2020
DHS/CBP/PIA-035(a) CBP Questions, Compliments and Complaints Management System	7/5/2020
DHS/CBP/PIA-049(a) License Plate Reader Technology	7/5/2020
DHS/USCIS/PIA-051(a) Case and Activity Management for International Operations (CAMINO)	7/6/2020
DHS/USCIS/PIA-082 Quality Assurance Database	7/6/2020
DHS/USCIS/PIA-083 Enterprise Collaboration Network	7/7/2020
DHS/ALL/PIA-027(d) Watchlist Service	7/11/2020
DHS/USSS/PIA-029 CID Retriever System	7/13/2020
DHS/CBP/PIA-064 Credibility Assessment and Polygraph Services	7/16/2020

Privacy Impact Assessments Published April 1– September 30, 2020	
DHS Component and System Name	**Date Published**
DHS/OBIM/PIA-003(a) Technical Reconciliation Analysis Classification System	7/16/2020
DHS/ALL/PIA-085 Counter-Unmanned Aircraft Systems	7/17/2020
DHS/ALL/PIA-080 DNA Collection	7/23/2020
DHS/CWMD/PIA-001 Medical and Public Health Information Sharing Environment	7/24/2020
DHS/CBP/PIA-053(a) U.S. Border Patrol Digital Forensics Programs	7/29/2020
DHS/FPS/PIA-001(d) Federal Protective Service Dispatch and Incident Record Management Systems	7/31/2020
DHS/CBP/PIA-012(b) E3	8/9/2020
DHS/CISA/PIA-035 National Cybersecurity Protection System (NCPS) - Core Infrastructure	8/10/2020
DHS/ICE/PIA-057 Angel Watch Program	8/10/2020
DHS/S&T/PIA-040 Data Analytics Technology Center (DATC) Laboratory System	8/12/2020
DHS/USSS/PIA-030 Comprehensive Financial Investigative System	8/13/2020
DHS/ALL/PIA-086 Counterintelligence Program	8/31/2020
DHS/ICE/PIA-058 Undercover Operations Unit Modernization	8/31/2020
DHS/ALL/PIA-043(a) Talent Acquisition	9/11/2020
DHS/ALL/PIA-050(b) Trusted Identity Exchange	9/17/2020
DHS/ALL/PIA-073(a) Electronic Discovery (eDiscovery) Tools	9/17/2020

System of Records Notices Published April 1, 2020 – September 30, 2020	
DHS Component and System Name	**Date Published**
DHS/USCIS-004 Systematic Alien Verification for Entitlements Program	5/27/2020
DHS/ALL-047 DHS Personnel and Visitors During a Declared Public Health Emergency	7/30/2020