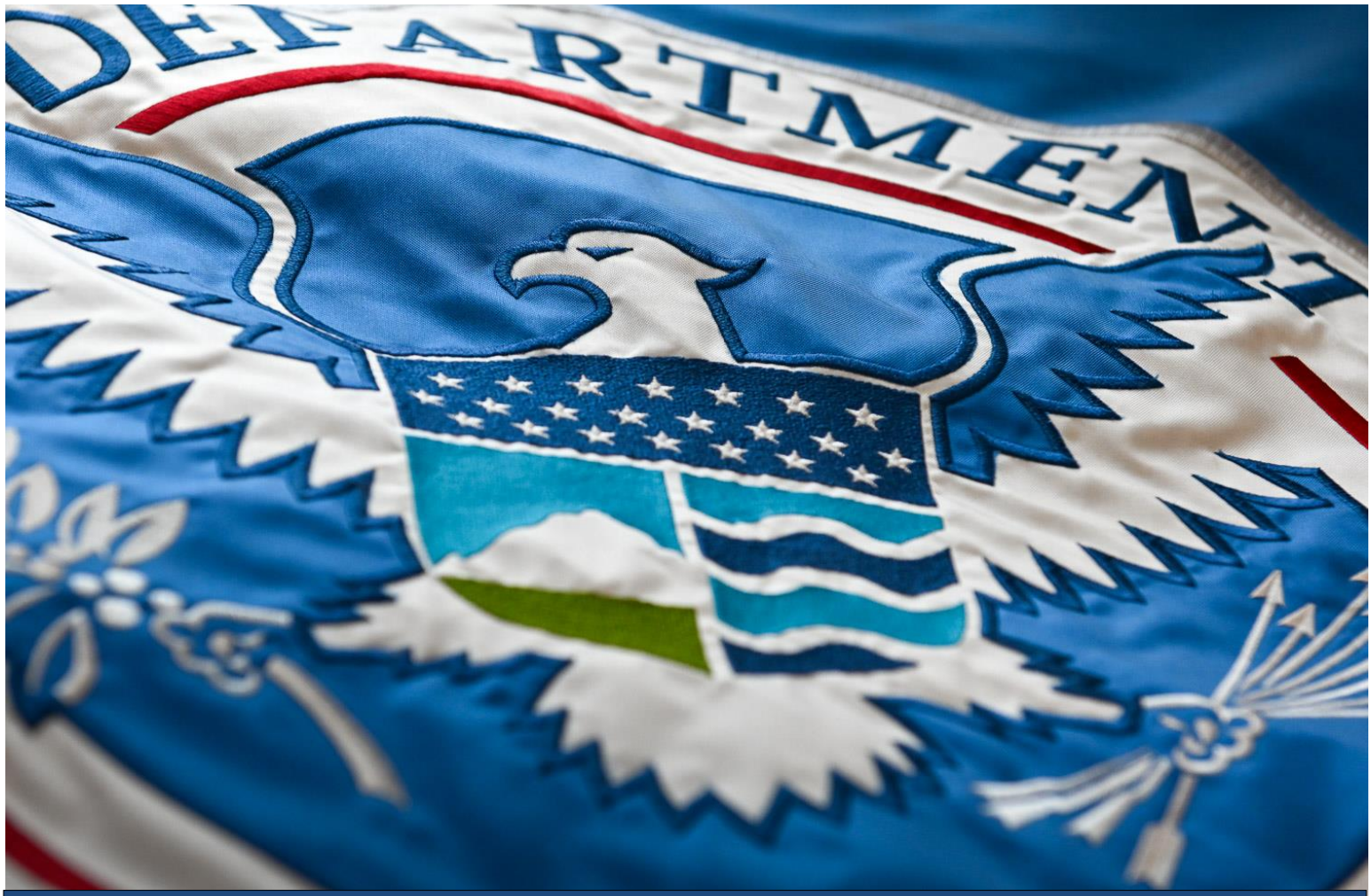


# Department of Homeland Security

## Privacy Office Fiscal Year 2021 Second Semi-Annual Report to Congress

*July 2023*

Homeland Security

# FOREWORD

*July 26, 2023*

I am pleased to present the *U.S. Department of Homeland Security Privacy Office Fiscal Year 2021 Second Semiannual Report to Congress*, covering the period April 1, 2021 – September 30, 2021.[1]

## Highlights

During the reporting period, the DHS Privacy Office:

- Completed 1,373 privacy reviews, including:
  - **1,054** Privacy Threshold Analyses;
  - **25** Privacy Impact Assessments; and
  - **Six** System of Records Notices and associated Privacy Act Exemptions.

## About the DHS Privacy Office

The DHS Chief Privacy Officer is the first statutorily mandated Chief Privacy Officer in the federal government. Section 2222, of the *Homeland Security Act of 2002*, charges the DHS Chief Privacy Officer with ensuring privacy protections are integrated into all DHS programs, policies, and procedures. The DHS Privacy Office's mission is to enable the Department to accomplish its mission while embedding and enforcing privacy protections and transparency in all DHS activities. The Chief Privacy Officer serves as the principal advisor to the DHS Secretary on privacy policy and establishes privacy policy for the Department.

The *Privacy Act of 1974* (Privacy Act), as amended, the *Freedom of Information Act* (FOIA), and the *E-Government Act of 2002*, requires transparent 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 privacy and FOIA policy implementation across the Department. The DHS Privacy Office undertakes these responsibilities in collaboration with DHS Component Privacy[2] and FOIA Officers, privacy points of contact, and program offices to implement privacy safeguards and enhance transparency across DHS.

Sincerely,

Mason C. Clutter
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.

[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 provided to the following Members of Congress:

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

The Honorable Rand Paul
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Richard J. Durbin
Chairman, Senate Committee on the Judiciary

The Honorable Lindsey Graham
Ranking Member, Senate Committee on the Judiciary

The Honorable Mark Warner
Chairman, Senate Select Committee on Intelligence

The Honorable Marco Rubio
Vice Chairman, Senate Select Committee on Intelligence

The Honorable Mark E. Green
Chairman, House Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, House Committee on Homeland Security

The Honorable James Comer
Chairman, House Committee on Oversight and Accountability

The Honorable Jamie Raskin
Ranking Member, House Committee on Oversight and Accountability

The Honorable Jim Jordan
Chairman, House Committee on the Judiciary

The Honorable Jerrold Nadler
Ranking Member, House Committee on the Judiciary

The Honorable Michael Turner
Chairman, House Permanent Select Committee on Intelligence

The Honorable James Himes
Ranking Member, House Permanent Select Committee on Intelligence

# DHS Privacy Office
# April 1, 2021- September 30, 2021
# Semiannual Report to Congress

## Table of Contents

# LEGISLATIVE LANGUAGE

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

"(f) Periodic Reports-

(1) In General –

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

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

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

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

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

(2) Contents –

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

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

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

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

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

[3] 42 U.S.C. § 2000ee-1(f).

# I. PRIVACY REVIEWS

The DHS Privacy Office reviews and evaluates Department programs, systems, and initiatives that collect personally identifiable information (PII) or otherwise have a privacy impact and provides mitigation strategies to reduce the privacy impact. For purposes of this report, privacy reviews include the following:

1. Privacy Threshold Analyses, as required by *DHS Privacy Policy and Compliance Directive 047-01*.
2. Privacy Impact Assessments, as required under the *E-Government Act of 2002*,[4] the *Homeland Security Act of 2002*,[5] and DHS policy.
3. System of Records Notices as required under the *Privacy Act of 1974*, as amended, and any associated Final Rules for Privacy Act exemptions;[6]
4. Privacy Act Statements, as required under the Privacy Act,[7] to provide notice to individuals at the point of collection.
5. Computer Matching Agreements, as required under the Privacy Act.[8]
6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*:[9]
7. Privacy Compliance Reviews, per the authority granted to the Chief Privacy Officer by the *Homeland Security Act of 2002*.[10]
8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) Exhibit 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board.
9. Information Technology Acquisition Reviews.[11]
10. Other privacy reviews at the discretion of the Chief Privacy Officer.

[4] 44 U.S.C. § 3501 note. *See also* OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003), *available at*: https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/.
[5] 6 U.S.C. § 142.
[6] 5 U.S.C. §§ 552a(e)(4), (j), (k). *See also* OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," 81 Fed. Reg. 94424 (Dec. 23, 2016), *available at*: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf.
[7] 5 U.S.C. § 552a(e)(3).
[8] 5 U.S.C. § 552a(o)-(u).
[9] 42 U.S.C. § 2000ee-3.
[10] The Chief Privacy Officer and DHS Privacy Office exercise 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 Privacy Compliance Reviews. 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 Privacy Compliance Review is designed as a constructive mechanism to improve a program's ability to comply with assurances made in existing privacy compliance documentation.
[11] Section 208 of the E-Government Act requires that agencies conduct a privacy impact assessment 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 ITAR requests to determine if the IT acquisitions require a new privacy impact assessment to identify and mitigate privacy risks or if they are covered by an existing DHS privacy impact assessment. In addition, the DHS Privacy Office reviews ITAR requests to ensure that appropriate language to safeguard 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:**<br>***April 1, 2021 – September 30, 2021*** | |
|---|---|
| ***Type of Review*** | ***Number of Reviews*** |
| Privacy Threshold Analyses | **1,054** |
| Privacy Impact Assessments | **25** |
| System of Records Notices and<br>associated Privacy Act Exemptions | **6** |
| Privacy Act (e)(3) Statements[12] | **117** |
| Computer Matching Agreements[13] | **3** |
| Data Mining Reports | **0** |
| Privacy Compliance Reviews | **0** |
| Privacy Reviews of IT and Program Budget Requests[14] | **0** |
| Information Technology Acquisition Reviews[15] (ITAR) | **168** |
| Other Privacy Reviews | 0 |
| ***Total Reviews*** | ***1,373*** |

[12] This total does not include all Components; several are permitted by the DHS Privacy Office to review and approve their own Privacy Act statements.
[13] Computer Matching Agreements are typically renewed or re-established.
[14] 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 semiannual reporting period.
[15] The DHS Privacy Office began conducting ITAR reviews in January 2016.

## Privacy Impact Assessments

The Privacy Impact Assessment process is one of the Department's key mechanisms to ensure that DHS programs and technologies embed privacy protections. In addition to completing privacy impact assessments for new systems and projects, programs, pilots, or information-sharing arrangements not currently subject to a privacy impact assessment, the Department also conducts a triennial review of existing privacy impact assessments to assess and confirm systems operate within original parameters. After the triennial review, the Department updates previously published privacy impact assessments to inform the public it has completed a review of affected systems.

As of September 30, 2021, 99 percent of the Department's *Federal Information Security Modernization Act* systems requiring a privacy impact assessment had a current privacy impact assessment. During the reporting period, the Office published 25 privacy impact assessments: 14 new and 11 updated.

All published DHS privacy impact assessments are available on the DHS Privacy Office website, www.dhs.gov/privacy.[16]

Below is a summary of significant privacy impact assessments published during the reporting period, including a hyperlink to the full text. A complete list of privacy impact assessments published during the reporting period is provided in the Appendix.

## New Privacy Impact Assessments

DHS/CISA/PIA-038 Use of Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification | Homeland Security *(May 14, 2021)*
DHS Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Division (CSD) established a process that permits CISA, pursuant to statutory authority, use of administrative subpoenas for cybersecurity vulnerability identification and notification. The process allows CISA to issue administrative subpoenas and receive customer or subscriber contact information from service providers to identify and notify owners or operators of covered systems and devices related to critical infrastructure with specific security vulnerabilities. CISA conducted this Privacy Impact Assessment because responses to administrative subpoenas include PII of individuals identified by subpoenaed service providers, such as Internet Service Providers (ISPs), as relevant points of contact.

DHS/ALL/PIA-090 Team Awareness Kit (TAK) | Homeland Security *(July 30, 2021)*
DHS is responsible for providing services and technologies to protect its workforce while increasing operational capabilities and enabling mission fulfillment. To this end, DHS enhanced and deployed Team Awareness Kit (TAK), a government-off-the-shelf application that enables near real-time location sharing and displays with operational personnel carrying devices. TAK is a geospatial infrastructure and situational awareness application providing enhanced situational awareness, navigation, surrounding land formation information, and data sharing. DHS conducted this Privacy Impact Assessment to discuss privacy risks associated with the deployment of this technology.

DHS/ALL/PIA-091 Family Reunification Task Force (FRTF) | Homeland Security
*(September 8, 2021)*

[16] Privacy impact assessments are unpublished when the subject matter is Law Enforcement Sensitive or involves a National Security System. Unpublished privacy impact assessments are on file with the DHS Privacy Office.

On February 2, 2021, President Biden signed Executive Order 1401 creating the President's Interagency Task Force on the Reunification of Families. DHS is the designated task force Chair and is joined by Department of State (DoS), Department of Health and Human Services (HHS), and the Department of Justice (DOJ) (collectively known as the Task Force). The Executive Order instructs the Task Force to identify and implement comprehensive strategies that bring families together and ensure children and parents who were intentionally separated from each other at the United States/Mexico border are provided support. The purpose of the Privacy Impact Assessment is to analyze privacy risks associated with PII as part of this effort and document mitigation strategies to ensure adequate protection of individual privacy.

## Updated Privacy Impact Assessments

DHS/ICE/PIA-023 Significant Event Notification System | Homeland Security
*(August 25, 2021)*
The Significant Event Notification system (SEN) is a reporting and law enforcement intelligence transmission tool developed by U.S. Immigration and Customs Enforcement (ICE), a component of the DHS. The ICE Office of Homeland Security Investigations (HSI) developed this system to create reports for ICE field and headquarters managers to provide timely information about critical incidents, activities, and events that involve or impact ICE field staff. The system also handles law enforcement intelligence communication from the ICE Office of Enforcement and Removal Operations (ERO) field offices to field and headquarters managers and ERO and HSI intelligence personnel. The original SEN Privacy Impact Assessment was published in 2010. ICE updated this Privacy Impact Assessment to reflect the current configuration of the program and to accurately document that SEN accesses and stores PII gathered during official ICE investigations or other law enforcement activities.

DHS/ICE/PIA-045(a) ICE Investigative Case Management (ICM) System | Homeland Security *(August 10, 2021)*
ICE has updated a major Information Technology (IT) system known as Investigative Case Management (ICM). ICM serves as the core tool for law enforcement case management for ICE Homeland Security Investigations (HSI) agents and personnel supporting the HSI mission. HSI conducts transnational criminal investigations to protect the United States against threats to national security and to bring to justice those seeking to exploit U.S. customs and immigration laws worldwide. ICE updated this Privacy Impact Assessment to reflect changes to Investigative Case Management's information-sharing framework with U.S. Customs and Border Protection (CBP), and to update the overview of the Privacy Impact Assessment to better reflect the user base and document a planned connection to HSI's Digital Records Manager (DRM).

## System of Records Notices

The Department publishes System of Records Notices consistent with requirements outlined in the *Privacy Act of 1974*, as amended.[17] The Department conducts assessments to ensure System of Records Notices remain accurate, up-to-date, and appropriately scoped; all System of Records Notices are published in the *Federal Register*; and all new System of Records Notices and significant changes to System of Records Notices are reported to OMB and Congress.

As of September 30, 2021, 100 percent of the Department's Privacy Act systems of records had an up-to-date System of Records Notice published in the *Federal Register*. During the reporting period, the Privacy Office published three new System of Records Notices and three associated Privacy Act rulemakings.

Below is a summary of a significant System of Records Notice published during the reporting period, and a hyperlink to the full text in the *Federal Register*. All published DHS System of Records Notices and Privacy Act rulemakings are available on the DHS Privacy Office website, https://www.dhs.gov/privacy. The System of Records Notices published during the reporting period are included in the Appendix.

## New System of Records Notice

DHS/OIDO-001 Office of the Immigration Detention Ombudsman System of Records
The purpose of this system is to allow DHS/OIDO to collect and maintain records to investigate potential violations of law, individual rights, standards of professional conduct, contract terms, or policy related to immigration detention by any officer or employee of CBP, ICE, or any contracted, subcontracted, or cooperating entity personnel.

## 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 was designed as a collaborative effort to help improve a program's ability to comply with existing privacy compliance documentation, including Privacy Impact Assessments, System of Records Notices, 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 Component Heads' responsibility to assist the Chief Privacy Officer in reviewing Component activities to ensure privacy protections are fully integrated into Component operations.

- A Privacy Compliance Review may result in a public report or internal recommendations, depending on the sensitivity of the program under review. The Privacy Office tracks the implementation of Privacy Compliance Review recommendations based on supporting evidence provided by the Component Privacy Office and/or the program office. A list of Privacy Compliance Review recommendations not yet implemented is posted on the Privacy Office website, www.dhs.gov/privacy, under Privacy Oversight, as well as public-facing Privacy Compliance Reviews.

[17] 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.

***Electronic System for Travel Authorization (ESTA) Privacy Compliance Review Update***

- Issued on November 7, 2017, the privacy compliance review report recommends that CBP consider developing and providing clearer instructions to ESTA applicants aimed at reducing inaccurate inclusion of non-identifier information in social media 'free-text' portions of the online application. In this reporting period, CBP confirmed the ESTA program no longer requires applicants to provide social media identifiers. The provision of social media information from applicants is expected to remain voluntary. CBP has not confirmed whether tagging in all its systems conforms to the caveat requirement in Directive 215-01-001.

***Science & Technology Directorate (S&T) Privacy Office Privacy Compliance Review Update***

- Issued on June 24, 2019, the privacy compliance review report recommends the S&T Privacy Office review and adopt DHS guidelines associated with records management. S&T reports the S&T Privacy Office completed an updated S&T Privacy Office File Plan. The work included the submission of a draft file plan to the S&T Records Management Liaison Officer in accordance with National Archives and Records Administration (NARA) requirements.

# II. ADVICE AND RESPONSES

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

## Privacy Policy Initiatives

**Privacy Policy Assessment Project**
The DHS Privacy Office continues to evaluate privacy policies,[18] directives, and instructions to ensure compliance with Departmental requirements, that technical content is updated and accurate, and policies are in line with updated legislative requirements. 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.

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

# III. TRAINING AND OUTREACH

## Mandatory Online Training

**139,307** DHS personnel completed a mandatory computer-assisted privacy awareness training course entitled, "Privacy at DHS: Protecting Personal Information." This course is required for all personnel when they join the Department, and annually thereafter.

**22,813** DHS personnel completed training on the operational use of social media 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

**6,336** DHS personnel attended instructor-led privacy training courses during this reporting period.

Additionally, the DHS Privacy Office either sponsored or provided a trainer for the following trainings:

- ***FOIA Training***: This periodic training is tailored to FOIA staff throughout the Department responsible for processing FOIA requests.
  - **March 2021 - Sunshine Week FOIA Training.**
    - 350 FOIA professionals attended the 2021 Sunshine Week FOIA Training Summit. The event provided a day of substantive training, including recorded remarks by Secretary Mayorkas and a Sunshine Awards ceremony led by Deputy Secretary Tien.
    - FOIA 9 on the 9s – a monthly training series on FOIA and privacy issues open to all DHS employees. Approximately 100 attendees per month attended this training.

- ***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 Component Privacy Officers also offer privacy training for new employees in their respective Components. In addition, the DHS Privacy Office provides a quarterly privacy training as part of the two-day course, *DHS 101*. It is offered to the DHS enterprise, but most attendees are from the Management Directorate.

- ***Privacy Briefings for Headquarters Staff*:** The DHS Privacy Office provides classroom privacy awareness training to Headquarters staff with an emphasis on identifying and resolving data vulnerabilities involving PII.

- ***Role-Based Training***: The DHS Privacy Office trains DHS Contracting Officers and Contracting Officers' Representatives on how to embed privacy protections into contracts. Acquisition management staff, which include the Heads of Contracting Activities, Component Acquisition Executives, and Component acquisition policy representatives, receive the training.

- ***DHS Privacy Office Boot Camp***: The DHS Privacy Office periodically trains new Component privacy staff on compliance best practices, including how to draft Privacy Threshold Analyses, Privacy Impact Assessments, and System of Records Notices.

- ***Reports Officer Course*:** The DHS Privacy Office provides privacy training to DHS Intelligence Enterprise officers who prepare intelligence reports.

- ***Raw Intelligence Release Authority Course:*** The DHS Privacy Office provides instruction to members of the DHS Intelligence Enterprise who seek the authority to approve raw intelligence for dissemination outside the federal government.
  - These are 60-90-minute-long briefings conducted for DHS Intelligence Enterprise employees and are part of longer courses taught by Intelligence and Analysis' **(**I&A) Intelligence Training Academy.

- ***Finished Intelligence Release Authority Course:*** The DHS Privacy Office provides instruction to members of the DHS Intelligence Enterprise who seek authority to approve finished intelligence products for dissemination outside the federal government.

- ***Security Specialist Course*:** The DHS Privacy Office provides privacy training every six weeks to participants of this week-long interagency training program.

## 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 Internet Security Agency (CISA)

- **275** CISA personnel completed instructor-led privacy training courses.

- **1,916** CISA personnel completed mandatory annual computer-assisted privacy awareness training: *Privacy at DHS: Protecting Personal Information*.

- **64** CISA personnel and contractors 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*, and any DHS Privacy Office adjudicated Component Social Media Operational Use Template(s). The audiences included personnel who support the CISA Integrated Operations Division and CISA Regional Operations teams.

  - On April 15, 2021, privacy analysts from the CISA Office of the Chief Privacy Officer conducted the Administrative Subpoena Process to 50 individuals across the Cybersecurity Division.

  - On June 10, 2021, Privacy Analysts from the CISA Office of the Chief Privacy Officer conducted privacy training for 75 individuals across the CISA Executive Secretariat regarding the privacy incident reporting and the safeguarding of PII in their use of the CISA Action Task Tracker (CATT).

  - On June 17, 2021, the CISA Office of the Chief Privacy Officer (OCPO)conducted a CISA-wide Townhall. The CISA OCPO discussed how the office represents the privacy interests of all individuals by promoting transparency, fairness, and equality by integrating full individual privacy protections into the management of a safe, secure, and resilient infrastructure. The Townhall

outlined CISA OCPO's organizational structure and the seven functional areas: compliance, oversight, policy and advice, training, privacy incident response, outreach, and civil rights and civil liberties. The Townhall was attended by over 800 CISA employees and contractors.

- On July 20, 2021, the CISA privacy officer delivered a keynote at a public virtual event for IT security practitioners on real-life applications of privacy risk and threat modeling.

- The CISA Office of the Chief Privacy Officer has two issues (June and September) of the quarterly privacy newsletter, CISA Privacy Update. The newsletter is distributed CISA-wide and posted on the CISA Office of Chief Privacy Officer's internal intranet page.

- On September 15, 2021, the CISA privacy officer delivered a keynote at a public virtual event for public sector digital government services on balancing privacy, security, and convenience for leveraging digital identity for government services.

**Federal Law Enforcement Training Centers (FLETC)**

- **859** FLETC personnel completed a mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

**Federal Emergency Management Administration (FEMA)**

- **175** FEMA personnel completed instructor-led privacy training.

- **11,846** FEMA personnel completed a mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

- **33** FEMA personnel 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*, and any DHS Privacy Office adjudicated Component Social Media Operational Use Template(s).

**Office of Intelligence and Analysis (I&A)**

- **489** I&A personnel completed a mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

**Office of the Chief Human Capital Officer (OCHCO)**

- **243** OCHCO personnel completed a mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

**Science and Technology Directorate (S&T)**

- **168** S&T personnel completed instructor-led privacy training courses.

- The S&T Privacy Office conducted privacy training for Program Managers (PMs) in S&T's Office of Mission & Capability Support (MCS). This training not only satisfied annual privacy training

requirements for attendees but also specifically addressed PMs' responsibilities to integrate privacy considerations and protections into their respective research, development, testing, and evaluation programs, projects, and activities.

- The S&T Privacy Office provided privacy training for the Homeland Security Systems Engineering and Development Institute (HSSEDI), a Federally Funded Research and Development Center (FFRDC). In addition to satisfying the annual privacy training requirement for attendees, this training also specifically addressed privacy requirements for the establishment of HSSEDI's information technology (IT) enclave, provided an overview of privacy protections within the IT enclave, and addressed privacy incident notification procedures.

**Transportation Security Administration (TSA)**

- **142** TSA personnel completed instructor-led privacy training courses.
  - 93 Information System Security Officers (ISSOs) attended training on preparing a Privacy Threshold Analysis.
  - 49 reviewers attended training on privacy considerations in processing reasonable accommodations requests.

- **19,176** TSA personnel completed a mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information.*

**295** TSA personnel 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*, and any DHS Privacy Office adjudicated Component Social Media Operational Use Template(s).

**U.S. Citizenship and Immigration Services (USCIS)**

- **650** USCIS personnel completed instructor-led privacy awareness training courses.

- **19,892** USCIS personnel completed a mandatory annual computer-based privacy awareness training course: *USCIS Privacy Awareness Training*.

- **195** USCIS personnel completed training on operational use of social media during the reporting period, as required by DHS Directive Instruction Number 110-01-001, *Privacy Policy for Operational Use of Social Media*.

- On September 14, 2021, the Office of US-VISIT conducted a briefing on OBIM and IDENT/HART to the USCIS Office of Privacy with the primary discussion focusing on the use of these systems and how privacy is built into their processes.

- USCIS Privacy conducted multiple briefings in June and July 2021, with USCIS leadership and personnel (employees and contractors) on best practices for emailing PII and Sensitive Personally Identifiable Information (SPII), disposal of PII/SPII for remote workers, and protecting PII/SPII when using collaboration tools and files stored on shared drives and ECN/SharePoint.

- USCIS Privacy published and disseminated the updated guidance memo *Privacy Guidance for Emailing PII and SPII*, on June 14, 2021. The guidance memo informed USCIS personnel of policy changes for transmitting email containing PII and SPII within and outside the DHS/USCIS network.

USCIS Privacy also published and disseminated updated Management Directive 140-002, *Privacy Program*, September 21, 2021.

- USCIS Privacy published and disseminated a quarterly newsletter entitled: *Privacy Chronicles on* September 23, 2021. This newsletter provides updates on current privacy policies and procedures, as well as privacy tips and current privacy news.

**U.S. Coast Guard (USCG)**

- **232** USCG personnel completed instructor-led privacy training courses.

- **24,022** USCG personnel completed a mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

- **86** USCG personnel completed training on operational use of social media during the reporting period, as required by DHS Directive Instruction Number 110-01-001, *Privacy Policy for Operational Use of Social Media*.

- USCG Privacy presented training to the bi-monthly CG Civilian Employee Orientation sessions, which were attended virtually by 232 newcomers. The forum focused on raising awareness of the importance of protecting personal information while assigned to the Department of Homeland Security. The privacy staff distributed and discussed relevant policies, as explained in the DHS factsheet "How to Safeguard SPII" and the Coast Guard Cybersecurity Manual, COMDTINST M5500.13 (series).

- USCG Privacy provided flyers emphasizing the requirements and instructions for encrypting electronic sensitive information sent to all Commands and remediating incidents involving unauthorized release of un-encrypted or non-password protected PII/SPII.

- USCG Privacy expanded a privacy awareness campaign service-wide by routinely composing informative notices, which are published on the USCG "Special notices" page on the USCG Portal and television screens located throughout the St. Elizabeths Campus, Washington, DC. One campaign was focused on awareness of encrypting/password-protecting emails with Sensitive PII.

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

- **2,254** CBP personnel attended in-person/virtual instructor-led privacy training courses.

- **52,558** CBP personnel completed a mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

- **22,014** CBP personnel 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*, and any DHS Privacy Office adjudicated Component Social Media Operational Use Template(s).
  - G1190001-01 – CBP Training for the Operational Use of Social Media – **503**
  - G0897003-42 – Personal Use of Social Media – **21,511**

- During the reporting period, the CBP Privacy Office remained constant in its customary proactive outreach and awareness efforts, which include targeted training in response to incident metrics.

Additionally, in this reporting period, CBP Privacy completed a rigorous virtual training initiative in support of agency Information Sharing initiatives. Training focused on personnel involved in the sharing of information in support of activities conducted by an appropriate Domestic Federal, State, Local, or Tribal authority charged with investigating or prosecuting a violation, or enforcing or implementing a law, rule, regulation, or order; or in support of the protection or safety of United States Government and/or CBP personnel, facilities, and/or operations. In addition to the training effort, CBP Privacy developed an abridged version of the training presentation which is available to all employees via the agency's Learning Management System.

- CBP Privacy continued to capitalize on the close partnership with the Office of Information Technology (OIT) – Cyber Defense Forensics Team through collaboration efforts by contributing "privacy equities" to various IT-Security messaging and certain aspects of the agency's data loss prevention tools.

- CBP Privacy is a standing participant in the CBP Office of Acquisitions' "Annual Lunch & Learn" training venue, designed to facilitate discussions of privacy inclusion in contract administration with respect to HSAR Class Deviation clauses and other privacy fundamentals.

- CBP Privacy continued efforts to heighten personnel privacy awareness and responsibilities throughout the agency through broadcasted privacy messaging by utilizing the agency's "Information Display System," main internal webpage (CBPnet), and other streams of information delivery. Messages were streamed monthly to include seasonal and holiday themed messages.

**U.S. Immigration and Customs Enforcement (ICE)**

- **2,266** ICE personnel completed instructor-led privacy training courses.

- **19,488** ICE personnel completed a mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

- **29** ICE personnel 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*.

- ICE Privacy conducted privacy training for Information System Security Officers (ISSOs). The discussion centered around the intersection of privacy and information security in system development lifecycles.

- ICE Privacy conducted privacy training about the use of third-party facial recognition services.

- ICE Privacy collaborated with the Office of the Chief Information Officer for training about communication strategy, telework status, encryption, and protecting PII and SPII.

**U.S. Secret Service (USSS)**

- **115** USSS personnel completed instructor-led privacy training courses.

- **4,102** USSS personnel completed a mandatory annual computer-assisted privacy awareness training course: *Privacy at DHS: Protecting Personal Information*.

- **296** USSS personnel completed training on operational use of social media during the reporting period, as required by DHS Directive Instruction Number 110-01-001, *Privacy Policy for Operational Use of Social Media.*

- On April 15, 2021, three USSS Inspectors were trained on Privacy Awareness as part of the USSS Inspection Process.

- On June 1, 2021, a Privacy Awareness Poster was created and disseminated to USSS Field Office Special Agents In Charge and Resident Agents in Charge Service-wide to post throughout their offices to enhance privacy awareness.

# IV. PRIVACY COMPLAINTS

The DHS Privacy Office is responsible for ensuring Department procedures are in place to receive, investigate, respond to and, 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 categorizes 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 System of Records Notices.
    a. *Example*: An individual alleges that a program violates Privacy Act or Departmental privacy policies 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. Redress also includes privacy-related complaints under the DHS Traveler Redress Inquiry Program (DHS TRIP). See below for more information.
    *a. Example:* An individual reports being misidentified during a credentialing process or traveler inspection at the border or screening at airports.
3. ***Operational:*** Issues related to general privacy concerns or other concerns not addressed in process or redress, but do not pertain to Privacy Act matters.
    a. *Example:* An individual alleges that personal health information was disclosed to a non-supervisor.
    b. *Example:* An individual alleges that physical screening and pat-down procedures at airports violate their privacy rights.
4. ***Referred*:** Complaints referred to another federal agency or external entity for handling.
    a. *Example:* A member of the public submits an inquiry regarding the individual's driver's license or Social Security number.

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 watchlist 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, 647 travelers marked that box. Upon review, none of the complaints received through TRIP described a privacy violation.

During the reporting period, the Department received **435** privacy complaints outside of the TRIP process.

| Type | CBP | CISA | FEMA | FPS | FLETC | ICE | TSA | USCIS | USCG | USSS | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ***Procedure*** | 83 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | **85** |
| ***Redress*** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** |
| ***Operational*** | 338 | 0 | 0 | 0 | 0 | 0 | 12 | 0 | 0 | 0 | **350** |
| ***Referred*** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | **0** |
| **TOTALS** | 421 | **0** | **0** | **1** | **0** | **0** | **13** | **0** | **0** | **0** | **435** |

**Procedure and Operational U.S. Customs and Border Protection (CBP) Examples**

**Procedure**

- Complainant, a U.S. citizen, stated that she was crossing the border in Rosarita when she told the CBP officer she was suffering a miscarriage. She was allegedly informed that there was no medical treatment available. The vehicle she was driving was impounded and she has not been able to get it back. She requested to speak to upper management. The case was transferred to the field office for review and follow up.

## Operational

- Complainant crossed into the United States at the Ambassador bridge where he alleged that a border agent harassed him regarding a previous arrest. Complainant stated that while the border agent was well within his right to ask questions that are relevant to the arrest at crossing, the border agent acted unprofessionally and laughed about the arrest with his colleague. Additionally, the complainant reported two minors were in the backseat and were exposed to his private information, making him feel uncomfortable and embarrassed. The case was transferred to field office for review and follow up to complainant.

- Complainant was detained at LAX and missed her connecting flight. The complainant stated that she approached the desk several times to ask about the detainment and express worry about missing the connecting flight. The complainant alleges that the front desk officer continued to share publicly her PII and made her answer personal questions out loud in front of everyone in the waiting room. The case was transferred to the field office for review and follow up to the complainant.

- Complainant was boarding a plane to Cancun for vacation with his pregnant wife and one year old child when he was detained. He reported he was interrogated in front of other passengers, and when he asked for a supervisor, the agent denied his request because the agent had not finished the interrogation. The complainant said the agent threatened the complainant by stating the complainant was uncooperative and would lose his Global Entry privilege. The complainant also said the agent made the complainant count all his money in front of other passengers. The complainant said he was the only Hispanic person boarding the plane and that no one else was detained. The case was transferred to the field office for review and follow up to the complainant.

# APPENDIX – PUBLISHED PRIVACY IMPACT ASSESSMENTS AND SYSTEM OF RECORDS NOTICES

| Privacy Impact Assessments<br>Published April 1, 2021 – September 30, 2021 | |
|---|---|
| **DHS Component and System Name** | **Date Published** |
| DHS/I&A/PIA-XXX Carbon Black | 4/8/2021 |
| DHS/CBP/PIA-070 Migrant Protection Protocol (MPP) Program | 5/2/2021 |
| DHS/USCIS/PIA-083 Enterprise Collaboration Network | 5/6/2021 |
| DHS/CBP/PIA-068 CBP One Mobile Application - TSA Functionality | 5/6/2021 |
| DHS/CBP/PIA-006 Automated Targeting System | 5/6/2021 |
| DHS/CBP/PIA-067 Unified Secondary | 5/7/2021 |
| DHS/CISA/PIA-038 Administrative Subpoenas for Cybersecurity Vulnerability Identification and Notification | 5/14/2021 |
| DHS/CBP/PIA-051 Mobile Passport Control (MPC) (Mobile Application) | 6/8/2021 |
| DHS/CBP/PIA-051(a) APC/MPC | 6/8/2021 |
| DHS/CBP/PIA-XXX TECS | 6/8/2021 |
| DHS/ICE/PIA-039(b) License Plate Readers | 6/11/2021 |
| DHS/OIG/PIA-002 Video Management System | 6/21/2021 |
| DHS/ALL/PIA-001 Immigration Detention Case Management System (ID-CMS) | 6/22/2021 |
| DHS/CWMD/PIA-002 Countering Weapons of Mass Destruction (CWMD) Biological Detection for the 21st Century (BD21) Technology Demonstration (TD) | 7/6/2021 |
| DHS/USCG/PIA-031 Palantir Data Analytics for CG-wide Use – COVID-19 | 7/20/2021 |
| DHS/CBP/PIA-052(a) Incident-Driven Video Recording Systems | 7/20/2021 |
| DHS/I&A/PIA-001 Analytic Exchange Program | 7/30/2021 |
| DHS/ALL/PIA-090 Team Awareness Kit | 7/30/2021 |
| DHS/CBP/PIA-012(c) E3 | 8/1/2021 |
| DHS/ICE/PIA-045(a) Investigative Case Management | 8/9/2021 |
| DHS/S&T/PIA-041 VTA- Office of Industry Partnership Portal | 8/20/2021 |
| DHS/ICE/PIA-023(a) Significant Event Notification | 8/25/2021 |
| DHS/S&T/PIA-042 DHS Federally Funded Research and Development Centers | 9/8/2021 |
| DHS/ALL/PIA-091 Family Reunification Task Force | 9/8/2021 |
| DHS/OIG/PIA-003 Data Analytics Cloud System | 9/29/2021 |

| System of Records Notices<br>Published April 1, 2021 – September 30, 2021 | |
|---|---|
| **DHS Component and System Name** | **Date Published** |
| DHS/CISA-005 Administrative Subpoenas for Cybersecurity Vulnerability | 4/5/2021 |
| DHS/S&T-003 National Bioforensic Analysis Center Laboratory Elimination Database | 5/9/2021 |
| DHS/OIDO-001 Office of the Immigration Detention Ombudsman (OIDO) | 9/3/2021 |