Department of Homeland Security

Privacy Office Semi-Annual Reports to Congress Covering October 2023 – September 2024

November 2025

Homeland Security

At the start of the Trump administration and my tenure on January 20, 2025, the DHS Privacy Office was delinquent on statutorily required reports. This backlog primarily resulted from a lack of prioritization of statutory reporting requirements by the Biden administration. While I have since approved and advanced several of these overdue reports through the approval process, the Department of Homeland Security Privacy Office is pleased to present the Semi-Annual Reports to Congress covering October 2023 – September 2024.

To return the Department to a regular reporting cadence and provide transparency into operations, this report covers two reporting periods: October 1, 2023 – March 31, 2024, and April 1, 2024 – September 30, 2024.

For additional information or inquiries, please contact the Department of Homeland Security Office of Legislative Affairs at (202) 447-5890 or via email at privacy@hq.dhs.gov.

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

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

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

The Honorable Charles E. Grassley
Chairman, Senate Committee on the Judiciary

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

The Honorable Tom Cotton
Chairman, Senate Select Committee on Intelligence

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

The Honorable Andrew Garbarino
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 Government Reform

The Honorable Stephen F. Lynch
Acting Ranking Member, House Committee on Oversight and Government Reform

The Honorable Jim Jordan

Chairman, House Committee on the Judiciary

The Honorable Jamie Raskin
Ranking Member, House Committee on the Judiciary

The Honorable Rick Crawford
Chairman, House Permanent Select Committee on Intelligence

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

Inquiries relating to this report may be directed to the DHS Office of Legislative Affairs at (202) 447-5890 or CongresstoDHS@hq.dhs.gov.

Sincerely,

Roman Jankowski
Chief Privacy Officer and Chief FOIA Officer
U.S. Department of Homeland Security

Department of Homeland Security Privacy Office
October 1, 2023, to September 30, 2024
Semiannual Reports to Congress

Table of Contents

LEGISLATIVE LANGUAGE 5
BACKGROUND 6
PRIVACY REVIEWS 8
- Privacy Impact Assessments 9
- System of Records Notices 14

ADVICE AND RESPONSES 15
- Privacy Compliance Reviews 15

COMPONENT PRIVACY AWARENESS INITIATIVES 15
- Cybersecurity and Internet Security Agency 15
- Federal Emergency Management Administration 16
- Federal Protective Service 17
- Office of Intelligence and Analysis 18
- Science and Technology Directorate 19
- Transportation Security Administration 19
- U.S. Citizenship and Immigration Services 20
- U.S. Coast Guard 21
- U.S. Customs and Border Protection 22
- U.S. Secret Service 24

PRIVACY COMPLAINTS 24
APPENDIX A– PUBLISHED PRIVACY IMPACT ASSESSMENTS 29

APPENDIX B – PUBLISHED SYSTEM OF RECORD NOTICES..... 30

LEGISLATIVE LANGUAGE

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*,[1] 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."

[1] 42 U.S.C. § 2000ee-1(f).

BACKGROUND

The Department of Homeland Security Chief Privacy Officer is the first statutorily mandated Chief Privacy Officer in the federal government. Section 222 of the *Homeland Security Act of 2002, as amended,* charges the Department of Homeland Security Chief Privacy Officer with ensuring privacy protections are integrated into all Department programs, policies, and procedures. The Department of Homeland Security Privacy Office's mission is to enable the Department to accomplish its mission while embedding and enforcing privacy protections and transparency in all Department activities.

The Department of Homeland Security Privacy Office collaborates with Component Privacy Officers,[2] Privacy Points of Contact,[3] and program offices to develop privacy policy, conduct oversight, respond to privacy incidents, and complete privacy compliance documentation.

DHS Privacy Office	Component Privacy Officers	Privacy Points of Contact
• Privacy Policy and Oversight Team • Privacy Compliance Team	• Cybersecurity and Infrastructure Security Agency (CISA) • Federal Emergency Management Agency (FEMA) • Office of Intelligence and Analysis (I&A) • Science and Technology Directorate (S&T) • Transportation Security Administration (TSA) • U.S. Citizenship and Immigration Services (USCIS) • United States Coast Guard (USCG/Coast Guard) • U.S. Customs and Border Protection (CBP) • U.S. Immigration and Customs Enforcement (ICE) • U.S. Secret Service (USSS)	• Countering Weapons of Mass Destruction Office (CWMD) • Office of the Chief Human Capital Officer (OCHCO) • Office of the Citizenship and Immigration Services Ombudsman (CISOMB) • Office of Health Security (OHS) • Office of Situational Awareness (OSA) • Office of Public Affairs (OPA) • Office of the Chief Security Officer (CSO) • Office of Immigration Statistics (OIS)

[2] The U.S. Department of Homeland Security policy requires every component to appoint a Privacy Officer to oversee privacy compliance, policy, and oversight activities in coordination with the Chief Privacy Officer. *See* U.S. DEPARTMENT OF HOMELAND SECURITY, DHS INSTRUCTION 047-01-005, COMPONENT PRIVACY OFFICER (2017), *available at* https://www.dhs.gov/publication/dhs-privacy-policy-instruction-047-01-005-component-privacy-officers.

[3] Privacy Points of Contact are assigned responsibility for privacy within their respective components, directorates, or programs, but they are not generally full-time privacy officers. Their privacy-related duties may be in addition to their primary responsibilities. Like Component Privacy Officers, Privacy Points of Contact work closely with component program managers and the U.S. Department of Homeland Security Privacy Office to manage privacy matters within the Department

DHS Privacy Office	Component Privacy Officers	Privacy Points of Contact
	• Office of Biometric Identity Management (OBIM) • Office of Inspector General (OIG) • Federal Law Enforcement Training Centers (FLETC) • National Vetting Center (NVC) • Federal Protective Service (FPS)	

PRIVACY REVIEWS

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, as amended, requires the Department of Homeland Security Privacy Office to provide information on the number and types of privacy reviews undertaken. The Department of Homeland Security Privacy Office reviews and evaluates Department regulations, rulemakings, technologies, policies, procedures, guidelines, programs, projects, or systems (including pilot activities), whether proposed or operational, that collect personal information or otherwise have a privacy impact and provides mitigation strategies to reduce the privacy impact. The accompanying chart below provides a detailed breakdown of these privacy reviews. For purposes of this report, privacy reviews include:

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 the Department of Homeland Security 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 of 1974*, as amended,[7] provide notice to individuals at the point of collection.
5. Computer Matching Agreements, as required under the *Computer Matching and Privacy Protection Act of 1988*.[8]
6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*.[9]
7. Privacy reviews of Information Technology and program budget requests, including the Office of Management and Budget's Exhibit 300s and Enterprise Architecture Alignment Requests through the Department of Homeland Security Enterprise Architecture Board.
8. Information Technology Acquisition Reviews.[10]
9. Other privacy reviews at the discretion of the Chief Privacy Officer.

---

[4] 44 U.S.C. § 3501 note. *See also* Office of Management and Budget Memorandum, M-03-22, Office of Management and Budget 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* Office of Management and Budget 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] Section 208 of the E-Government Act requires that agencies conduct a privacy impact assessment before procuring information technology that collects, maintains, or disseminates information that is in an identifiable form. The U.S. Department of Homeland Security meets this requirement in part by participating in the Information Technology Acquisition Review process. The Privacy Office reviews Information Technology Acquisition Review requests to determine if the information technology acquisitions require a new privacy impact assessment to identify and mitigate privacy risks or if they are covered by an existing U.S. Department of Homeland Security privacy impact assessment. In addition, the Privacy Office reviews Information Technology Acquisition Review requests to ensure that appropriate language to safeguard personally identifiable information and sensitive personally identifiable information 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:		
Type of Review	***Number of Reviews*** **1st Half of FY 2024** ***October 1, 2023 – March 31, 2024***	***Number of Reviews*** **2nd Half of FY 2024** ***April 1, 2024 – September 30, 2024***
Privacy Threshold Analyses	1106	1291
Privacy Impact Assessments	13	11
System of Records Notices and associated Privacy Act Exemptions	0	2
Privacy Act (e)(3) Statements[11]	154	182
Computer Matching Agreements[12]	4	0
Data Mining Reports	0	0
Privacy Reviews of IT and Program Budget Requests[13]	0	51
Information Technology Acquisition Reviews[14]	382	550
Other Privacy Reviews	0	0
Total Reviews	***1,659***	***2,087***

Privacy Impact Assessments

The Privacy Impact Assessment process is one of the Department's key mechanisms to ensure that the U.S. Department of Homeland Security programs and technologies embed privacy safeguards. In addition to completing privacy impact assessments for new systems, projects, programs, pilots, or information-sharing arrangements not currently subject to a privacy impact assessment, the Department also conducts a

[11] This total does not include all Components; several are permitted by the U.S. Department of Homeland Security Privacy Office to review and approve their own Privacy Act statements.

[12] Computer Matching Agreements 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 semiannual reporting period.

[14] The U.S. Department of Homeland Security Privacy Office began conducting Information Technology Acquisition Reviews in January 2016.

triennial review of existing privacy impact assessments to assess and confirm systems' operation within original parameters. After each triennial review, the Department updates previously published privacy impact assessments to notify the public that a review of the affected systems have been completed.

As of September 30, 2024, all the Department's systems subject to the Federal Information Security Modernization Act have a current privacy impact assessment.

All published privacy impact assessments are available on the U.S. Department of Homeland Security Privacy Office website, www.dhs.gov/privacy.[15]

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

New Privacy Impact Assessments

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

DHS/ALL/PIA-097 Use of Conditionally Approved Commercial Generative Artificial Intelligence Tools | Homeland Security *(November 2023)*
In accordance with the Secretary of Homeland Security's recent announcement on the Department's use of Artificial Intelligence, the Office of the Chief Information Officer, in coordination with the Science and Technology Directorate, Privacy Office, Office for Civil Rights and Civil Liberties, and Office of the General Counsel, is leading the Department's efforts to ensure responsible use of Artificial Intelligence while fulfilling the Department's mission and supporting its workforce. As part of this effort, the Office of the Chief Information Officer, is working to advance specific mission applications of Artificial Intelligence across the Department, and address ways in which the workforce may use conditionally approved commercially available generative Artificial Intelligence tools (i.e., tools not procured for use for specific Department missions) for certain aspects of their work. Generative Artificial Intelligence is the class of Artificial Intelligence models that emulate the structure and characteristics of input data to generate novel synthetic content (i.e., outputs). This can include images, videos, audio, text, code, and other types of digital content. This Privacy Impact Assessment analyzes the Department's use of conditionally approved generative Artificial Intelligence tools.

DHS/ICE/PIA-064 Immigration and Customs Enforcement Operational Use of Publicly Available Information Including Social Media Information for Law Enforcement Investigations | Homeland Security *(November 2024)*
The U.S. Immigration and Customs Enforcement has a statutory mission to enforce immigration laws and combat transnational crime. To support this mission, personnel collect publicly available information, including data from the internet and social media platforms. Some of this information may include personally identifiable data. This Privacy Impact Assessment addresses the collection and use of publicly available information for law enforcement investigations, with further analysis of data maintenance and sharing covered in the respective Privacy Impact Assessments for the systems where the data is stored.

DHS/S&T/PIA-044 Cloud-based Biometric Analytic Environment | Homeland Security *(March 2024)* The Science and Technology Directorate's Biometrics and Identity Technology Center (BI-TC) has developed

[15] 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 Department of Homeland Security Privacy Office.

the Cloud-based Biometric Analytic Environment to support research, development, testing, and evaluation of biometric tools. This system assesses the performance of biometric collection, matching, and other tools used by the U.S. Department of Homeland Security, using biometric, biographic, and demographic data from Components. The Privacy Impact Assessment addresses the privacy risks and mitigations associated with the use and maintenance of personally identifiable information within this system.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

DHS/OIG/PIA-004 TeamMate Application | Homeland Security *(May 2024)*
The Office of Inspector General conducts independent audits, inspections, evaluations, and investigations to prevent fraud, waste, and abuse, and to promote efficiency within the U.S. Department of Homeland Security programs and activities. These functions are carried out through the Office of Audits and the Office of Inspections and Evaluations. TeamMate, a Windows-based audit management application, is installed on servers at the Office of Inspector General's primary data center and provides a common platform for documenting, sharing, reviewing, and tracking work throughout the lifecycle of an audit, inspection, or evaluation. Auditors and inspectors collect information via work papers, interviews, and on-site visits, which is then uploaded into TeamMate. They may request and receive personally identifiable information and sensitive personally identifiable information when relevant to the review, which may be included in supporting documents provided to or obtained by the Office of Inspector General.

DHS/FEMA/PIA-059 Individual Assistance (IA) Systems | Homeland Security *(August 2024)*
The Individual Assistance Division within the Federal Emergency Management Agency's Office of Response and Recovery manages the Federal Emergency Management Agency Individual Assistance programs. The Individual Assistance programs rely on a portfolio of information technology systems and multiple applications to provide disaster recovery assistance, such as food and shelter, to individuals under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), as amended, following a presidentially declared disaster. This Privacy Impact Assessment focuses on the information technology systems and supporting subsystems used by the Individual Assistance programs. The Individual and Households Program is covered in a separate, forthcoming Privacy Impact Assessment.

DHS/CBP/PIA-081 Criminal Case Management System (CCMS) | Homeland Security *(August 2024)*
The U.S. Customs and Border Protection Criminal Case Management System serves as the primary investigative case management system for all criminal cases in various stages of investigation across U.S. Customs and Border Protection. The Criminal Case Management System allows U.S. Customs and Border Protection to record, maintain, link, coordinate, de-conflict, and share timely criminal case information, as well as centrally manage evidence, document criminal case development, and track prosecutorial and investigative outcomes. U.S. Customs and Border Protection conducted this Privacy Impact Assessment to assess the potential privacy risks and mitigation measures associated with Criminal Case Management System because it collects, stores, and uses personally identifiable information about members of the public.

DHS/USSS/PIA-033 USSS Use of Facial Recognition Technology | Homeland Security *(September 2024)*
The U.S. Secret Service conducted this Privacy Impact Assessment because Secret Service personnel may use facial recognition technology during law enforcement activities within the agency's jurisdiction. The use of this technology requires the collection and maintenance of personally identifiable information, such as facial images, to assist with developing investigative leads related to counterfeiting, financial crimes, and cyber-enabled crimes. In authorized criminal investigations, personnel may utilize the Office of Biometric Identity Management's Automated Biometric Identification System and other government facial

recognition technology for database searches or one-to-one comparisons to generate leads. The Secret Service does not use commercially provided facial recognition services. This Privacy Impact Assessment will address the potential privacy risks associated with using facial recognition technology for criminal investigative purposes.

Updated Privacy Impact Assessments

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

DHS/CBP/PIA-014(b) Centralized Area Video Surveillance System *(October 2023)*
U.S. Customs and Border Protection uses the Centralized Area Video Surveillance System, which includes cameras and microphones to record video and audio of persons involved in incidents or disturbances related to law enforcement at the border, including inspection areas, during attempts to enter or gain admission to the United States. The system collects and disseminates personally identifiable information in the form of video and audio recordings. U.S. Customs and Border Protection updated this Privacy Impact Assessment to document the National Archives and Records Administration-approved records retention schedule for the system.

DHS/CBP/PIA-051(b) Mobile Passport Control *(November 2023)*
U.S. Customs and Border Protection developed the Automated Passport Control and Mobile Passport Control programs to streamline the processing of eligible travelers entering the United States. These programs allow travelers to voluntarily submit their travel document, photograph, and customs declaration information using a self-service kiosk or a mobile device application, reducing passport control inspection time and overall wait time. U.S. Customs and Border Protection published this Privacy Impact Assessment to document the retirement of the Automated Passport Control and the expansion of Mobile Passport Control.

DHS/TSA/PIA-046(d) TDC Automation Using Facial Identification *(November 2023)*
The Transportation Security Administration, in partnership with U.S. Customs and Border Protection, has expanded the use of facial identification technology to enhance identity verification at Transportation Security Administration checkpoints. The latest proof of concept uses a Credential Authentication Technology device equipped with a camera and biometric matching services from U.S. Customs and Border Protection's Traveler Verification Service to verify the identities of travelers who opt-in during check-in at Detroit Metropolitan Wayne County Airport in partnership with Delta Airlines. This Privacy Impact Assessment has been updated to document the potential use of alternate devices, such as tablets, at some airports to test their capability to perform Credential Authentication Technology functions.

DHS/S&T/PIA-031(a) Select Agent Inventory *(February 2024)*
The Select Agent Inventory is a database and workflow system used by the Science & Technology Directorate's Plum Island Animal Disease Center to support the Federal Select Agent Program, which oversees the possession, use, and transfer of biological select agents and toxins posing severe threats to public, animal, or plant health. The Science & Technology Directorate updated this Privacy Impact Assessment to document the inclusion of additional health clinic data and the integration of a Training Database into the Select Agent Inventory system. These updates aim to automate manual processes within the Plum Island Animal Disease Center Occupational Health Clinic. This update also addresses the privacy risks associated with the additional collection and use of personally identifiable information, accessible only to the Science & Technology Directorate, to support the new Occupational Health Clinic Medical Database and the integrated Training Database.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

DHS/CBP/PIA-007(i) Electronic System for Travel Authorization (ESTA) *(April 2024)*
The Electronic System for Travel Authorization is an application and screening system used to determine whether citizens and nationals from Visa Waiver Program countries are eligible to travel to the United States. U.S. Customs and Border Protection published this Privacy Impact Assessment update for the Electronic System for Travel Authorization to provide notice and assess privacy risks associated with recent enhancements, including sharing national identifier numbers from Electronic System for Travel Authorization applicants with the issuing country to obtain information as part of the International Biometric Information Sharing Program, and updates to the Electronic System for Travel Authorization mobile application.

DHS/USCIS/PIA-075(a) RAILS (*May 2024)*
The U.S. Citizenship and Immigration Services developed RAILS (not an acronym) to enable the U.S. Department of Homeland Security and authorized U.S. Citizenship and Immigration Services personnel to request immigration files, maintain an accurate file inventory, and track the location of paper and electronic immigration records through a web-based system. RAILS allows users to order, transfer, and receive official records associated with an Alien Number or receipt number. This updated Privacy Impact Assessment identifies new uses of RAILS, including the Person Centrix Query Service and IMPACT (not an acronym), through the Enterprise Citizenship and Immigration Services Centralized Operational Repository, as well as new connections to U.S. Citizenship and Immigration Services systems such as Person Centric Identity Services, the U.S. Citizenship and Immigration Services Freedom of Information Act Immigration Records System, and Content Management Services. The update also outlines the sharing of Alien File information with external systems, including the National Archives and Records Administration's Archival Records Center Information System and Iron Mountain's Records Manager system.

DHS/USSS/PIA-017(b) Forensics Service Division System *(May 2024)*
The U.S. Secret Service Forensic Services Division System provides a suite of applications that support the Secret Service mission. These applications offer evidence and case tracking, automated handwriting recognition, and digital examination and storage of fingerprints and palm prints. This Privacy Impact Assessment update discusses the sharing of personally identifiable information with the Office of Biometric Identity Management's Automated Biometric Identity System and the National Capital Regional Automated Fingerprint Identification System, which includes Fairfax County, Virginia; Washington, D.C.; and Montgomery and Prince George's Counties, Maryland. Additionally, it documents how Forensic Services Division examiners can route Live-Scan collected known fingerprint records and latent prints through the Federal Bureau of Investigation's Next Generation Identification system for searching.

DHS/CBP/PIA-007(j) Electronic System for Travel Authorization (ESTA) *(July 2024)*
The Electronic System for Travel Authorization is used to determine whether citizens and nationals from Visa Waiver Program countries are eligible to travel to the United States. U.S. Customs and Border Protection published this Privacy Impact Assessment update to provide notice of and assess the privacy risks associated with recent enhancements to the Electronic System for Travel Authorization, including the expanded collection of an applicant's photograph.

DHS/CBP/PIA-006(e) Automated Targeting System *(August 2024)*

U.S. Customs and Border Protection operates the Automated Targeting System. The Automated Targeting System is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments. U.S. Customs and Border Protection updated this Privacy Impact Assessment to provide an addendum for Commercially Available Tools.

DHS/FLETC/PIA-003(a) eFLETC *(September 2024)*
The Federal Law Enforcement Training Centers has implemented eFLETC as a virtual learning management environment supporting law enforcement training for federal, state, local, tribal, territorial, and international law enforcement officers. The eFLETC serves as a scheduling, instructional delivery, and records system for up to 14,000 students. The eFLETC automates and integrates processes to improve the efficiency of administrative support functions for online student training and registration, content delivery, and course analytics. The Federal Law Enforcement Training Centers conducted this Privacy Impact Assessment update to clarify the information collected in eFLETC, to include the removal of Social Security numbers.

System of Records Notices

The Department publishes System of Records Notices consistent with requirements outlined in the *Privacy Act of 1974*, as amended.[16] The Department conducts assessments to ensure System of Records Notices remain accurate, up-to-date, and appropriately scoped. System of Records Notices are published in the *Federal Register*. New System of Records Notices and those with significant changes are reported to the Office of Management and Budget and Congress.

As of September 30, 2024, 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*. Below is a summary of System of Records Notices published during the reporting period.

DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records *(July 2024)*
U.S. Immigration and Customs Enforcement collects, uses, and maintains Criminal Arrest Records and Immigration Enforcement Records to support the identification, apprehension, and removal of aliens unlawfully entering or present in the United States, including fugitive aliens, in violation of the Immigration and Nationality Act. U.S. Immigration and Customs Enforcement also uses these records to identify and arrest individuals who violate federal laws enforced by the U.S. Department of Homeland Security. U.S. Immigration and Customs Enforcement reissued this System of Records Notice to update the system's purpose, add new categories of individuals and records, and modify, remove, and propose new routine uses. Additionally, the notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This modified system will be included in the Department's inventory of record systems.

DHS/FEMA-008 Disaster Recovery Assistance Files System of Records *(September 2024)*
The purpose of this system is to register applicants seeking disaster assistance from the Federal Emergency Management Agency after a Presidential major disaster declaration or emergency, or when a declaration is imminent; verify applicant information for the Individuals and Households Program; determine eligibility; correspond with and refer applicants to available sources of disaster assistance; and inspect damaged

[16] 5 U.S.C. §§ 552a(e)(4), (j), (k). *See also* Office of Management and Budget 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.

property. Additional purposes include identifying and implementing measures to reduce future disaster damage, preventing or correcting duplication of federal efforts and benefits, identifying possible fraudulent activity, identifying assistance provided in error or misused by the applicant, and assessing customer satisfaction. The Federal Emergency Management Agency updated this system of records notice to add or modify several routine uses and update the categories of records. This modified system will be included in the U.S. Department of Homeland Security's inventory of record systems.

ADVICE AND RESPONSES

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, as amended, requires the Department of Homeland Security Privacy Office to describe the advice provided and the corresponding response. The Privacy Office offers this advice through recommendations.

Privacy Compliance Reviews

The Department of Homeland Security Privacy Office exercises its oversight function under 6 U.S.C. § 142 to ensure the Department's use of technology sustains, and does not erode, privacy protections, primarily by conducting Privacy Compliance Reviews. The Privacy Office collaborates with Component Privacy Officers and the managers of systems or programs under review to assess compliance with privacy laws, regulations, and Departmental policies. Through these reviews, the Privacy Office develops recommendations and works with Component Privacy Officers to ensure compliance or enhance privacy protections. The Privacy Office oversaw the implementation of 14 recommendations, resulting in the closure of four Privacy Compliance Reviews.

COMPONENT PRIVACY AWARENESS INITIATIVES

Cybersecurity and Internet Security Agency

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

- The Cybersecurity and Infrastructure Security Agency's Office of Privacy, Access, Civil Liberties, and Transparency organized a Privacy Incident Preliminary Training and Tabletop Exercise. Privacy analysts led a training for 27 individuals and a tabletop exercise for 113 participants, focusing on identifying privacy incidents, reporting processes, and investigations through two scenarios.
- The Cybersecurity and Infrastructure Security Agency's Office of Privacy, Access, Civil Liberties, and Transparency conducted a training session for 51 individuals in the Office of the Chief Information Officer on the privacy compliance process and document drafting.
- The Cybersecurity and Infrastructure Security Agency's Office of Privacy, Access, Civil Liberties, and Transparency reported that 207 personnel completed the mandatory annual computer-assisted privacy awareness training, "Privacy at the Department of Homeland Security: Protecting Personal Information".
- The Cybersecurity and Infrastructure Security's Agency Office of Privacy, Access, Civil Liberties, and Transparency delivered a privacy briefing during New-Employee Orientation to 298 new employees.
- The Cybersecurity and Infrastructure Security Agency's Office of Privacy, Access, Civil Liberties, and Transparency reported that two personnel and contractors from Region IX completed training on the

operational use of social media, as required by the U.S. Department of Homeland Security Directive Instruction Number 110-01-001, Privacy Policy for Operational Use of Social Media.

- The Cybersecurity and Infrastructure Security Agency's Office of Privacy, Access, Civil Liberties, and Transparency reported that ten personnel and contractors from the Integrated Operations Division completed the operational use of social media training, in compliance with the U.S. Department of Homeland Security Directive Instruction Number 110-01-001 and any relevant Privacy Office adjudicated Component Social Media Operational Use Templates.
- The Cybersecurity and Infrastructure Security Agency's Office of Privacy, Access, Civil Liberties, and Transparency produced three issues of its quarterly privacy newsletter (December, March, and June), which was distributed agency-wide and posted on the Office's internal intranet page.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

- The Cybersecurity and Infrastructure Security Agency's Office of Privacy, Access, Civil Liberties, and Transparency provided privacy awareness training to 309 employees during their new employee orientation.
- The Cybersecurity and Infrastructure Security Agency's Office of Privacy, Access, Civil Liberties, and Transparency provided Operational Use of Social Media for Situational Awareness Purposes Rules of Behavior training to 59 employees.
- The Cybersecurity and Infrastructure Security's Agency Office of Privacy, Access, Civil Liberties, and Transparency conducted a privacy incident tabletop exercise with key stakeholders throughout the agency, simulating both minor and major incidents, with the participation of 110 employees.

Federal Emergency Management Administration

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

- The Federal Emergency Management Agency Privacy Office conducted a training in collaboration with the Recovery Reporting and Analytics Division Privacy for 40 members of the New Mexico Joint Field Office. The training covered privacy topics such as handling personally identifiable information, sensitive personally identifiable information, and information sharing.
- The Federal Emergency Management Agency Privacy Office conducted a training for 21 onboarding contractors in the Office of Policy and Program Analysis. This session focused on handling personal information, privacy policies, data sharing agreements, incident reporting and prevention, and aggregated data.
- The Federal Emergency Management Agency Privacy Office conducted a training for 28 staff members of the Hermit's Peak Claims Office under the Office of Response and Recovery. Topics included handling personal information, the distinction between Need-to-Know and Routine Use, privacy compliance documents, and incident reporting and prevention strategies.
- The Federal Emergency Management Agency Privacy Office hosted a brown bag session for 130 members of the Office of Business Management under Resilience. This session covered handling personal information, Need-to-Know vs. Routine Use, SharePoint and Outlook guidance, and incident reporting and prevention strategies.
- The Office of Chief Counsel, Information Law Branch, conducted Privacy Act training for 50 attorneys as part of the Introduction to Federal Emergency Management Agency Office of Chief Counsel Field Operations training.
- The Office of Chief Counsel, Information Law Branch, conducted five trainings on privacy compliance for Federal Emergency Management Agency Legal Introductory Training for Executives classes.

- The Office of Chief Counsel, Information Law Branch, provided a privacy briefing on new developments and innovations at the Office of Chief Counsel All Hands meeting for 300 attorneys.
- The Office of Chief Counsel, Information Law Branch, presented privacy primer training to the new Office of Response and Recovery attorneys.
- The Office of Chief Counsel, Information Law Branch, conducted training for General Law Attorneys on new Privacy Threshold Analyses and other privacy developments, including a panel discussion with the Federal Emergency Management Agency Privacy Office and Federal Emergency Management Agency Program experts.
- The Office of Chief Counsel, Information Law Branch, provided a privacy workshop training for 370 Federal Emergency Management Agency Region 1 and Joint Field Office personnel.
- The Office of Chief Counsel, Information Law Branch, hosted a workshop for the Office of Chief Counsel Alternative Dispute Resolution attorneys and staff on drafting and reviewing Privacy Threshold Analysis.
- The Office of Chief Counsel, Information Law Branch, presented privacy primer training to new Office of Response and Recovery attorneys.
- The Federal Emergency Management Agency Privacy reported that 9,468 personnel completed the mandatory annual computer-assisted privacy awareness training course: "Privacy at the Department of Homeland Security: Protecting Personal Information."

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

- The Federal Emergency Management Agency Privacy Office partnered with three program offices to coordinate six Privacy, Data Sharing, and Records Management Working Group meetings. This initiative led to the creation of a privacy and data sharing resource hub and a community of subject matter experts, empowering staff and external partners to enhance their knowledge, collaborate, and take on more responsibility in the privacy and data sharing space.
- The Federal Emergency Management Agency Privacy Office coordinated six Information Sharing Community of Practice meetings, providing a platform for the community to connect, share updates, and discuss topics related to privacy, data and information sharing, and information management.
- The Federal Emergency Management Agency Privacy Office provided Privacy Foundations training to the following program offices, focusing on topics such as personally identifiable information, the Privacy Act of 1974, Fair Information Practices and Principles, privacy legislation, and incident prevention and reporting:
    - Office of Response and Recovery Individual Assistance Community Services: 14 individuals in April 2024
    - Office of Response and Recovery Field Operations Directorate: 214 individuals in April 2024
    - Region 9 Joint Field Office: 176 individuals in April 2024
    - Office of the Chief Security Officer: 157 individuals in May 2024
    - Flood Insurance and Mitigation Administration: 43 individuals in May 2024
- The Federal Emergency Management Agency Privacy Office provided Privacy Foundations and Acquisitions Overview training to the Office of the Chief Procurement Officer for 23 individuals.

Federal Protective Service

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

- The Federal Protective Service Privacy and the Freedom of Information Office provided six monthly privacy awareness briefings at the New Employee Orientation onboarding sessions presented by the Federal Protective Service Human Capital Management Directorate. The training, attended by 102 new

employees, included instructor-led sessions on privacy compliance, privacy oversight, and Freedom of Information Act processes at the Federal Protective Service and the Department, in addition to the computer-based training required of all new U.S. Department of Homeland Security employees.

- The Federal Protective Service Privacy and Freedom of Information Office continued to offer ad-hoc 'train-the-trainer' Privacy Act and Freedom of Information Act sessions for four internal staff members, aimed at raising awareness of the U.S. Department of Homeland Security Privacy Policy. These sessions were designed to enhance the skills of staff in the Federal Protective Service Privacy and Office of General Counsel, enabling them to share knowledge within Federal Protective Service divisions. Additionally, privacy compliance kick-off meetings, led by Federal Protective Service Privacy Analysts, were held prior to new projects or programs to inform project managers of their privacy responsibilities and address questions about the privacy compliance documentation process.
- The Federal Protective Service Privacy and the Freedom of Information Office developed and presented role-based Privacy Act and Freedom of Information Act briefings for Federal Protective Service Law Enforcement personnel who participated in the Body Worn Camera initiative. The Federal Protective Service Privacy team participated in six in-person annual law enforcement sessions at the Federal Protective Service Bren Mar training facility, in Chicago, and in New York, where approximately 215 inspectors and officers were in attendance.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

- The Federal Protective Service Privacy and the Freedom of Information Office coordinated with the Human Capital Operations Division to present Privacy and Freedom of Information Act Awareness Training during the monthly New Employee Orientation to 115 new Federal Protective Service employees, including law enforcement personnel attending Federal Protective Service training programs at the Federal Law Enforcement Training Centers and contractors assigned to headquarters and regional locations.

Office of Intelligence and Analysis

- The Office of Intelligence and Analysis is obligated under its Intelligence Oversight Program to ensure that all personnel receive training on the Intelligence Oversight Guidelines within 30 days of starting employment and annually thereafter. This training covers privacy requirements in the context of Executive Order 12333 intelligence functions. This training is provided live, typically twice a month, to new hires, including both federal employees and contractors.
- The Office of Intelligence and Analysis provided the “Privacy at DHS: Protecting Personal Information” training, which is available on the training platform maintained by the Office of Intelligence and Analysis’s Intelligence Training Academy. A total of 939 individuals completed the “Privacy at the Department of Homeland Security” training online through this platform.
- The Office of Intelligence and Analysis invited the Headquarters Privacy Office to speak directly to new federal intelligence professionals as part of its quarterly orientation program, along with other DHS oversight offices involved in reviewing intelligence products.
- The Branch Chief of the Privacy and Intelligence Oversight Branch, who serves as the Office of Intelligence and Analysis Privacy Officer, provided an additional presentation on privacy concepts and compliance documentation to 25 key stakeholders.

Science and Technology Directorate

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

- The Science and Technology Directorate Privacy Office conducted joint training with Procurement Review Officials within the Science and Technology Office of the Chief Information Officer, Office of the Chief Security Officer, Privacy Office, and Contract Acquisition Program Support. This session trained 257 employees on new privacy and security requirements for contracts, based on recently updated U.S. Department of Homeland Security acquisition regulations for Controlled Unclassified Information.
- The Science and Technology Directorate Privacy Office briefed the Science and Technology Office of Enterprise Services Executive Team on all functions of the Science and Technology Privacy Program. This training followed changes in the organizational structure of Science and Technology Privacy and its integration into the Office of Enterprise Services team.
- The Science and Technology Directorate Privacy Office conducted a training session for the new Office of University Programs Arctic Domain Awareness Center, covering shared privacy responsibilities, privacy sensitivity, and safeguarding personal information, and highlighting the updated Office of University Programs Terms and Conditions.
- The Science and Technology Directorate Privacy Office trained 12 new staff members of the System of Systems Operational Analytics team, on handling personal information and developing privacy compliance documentation.
- The Science and Technology Directorate Privacy Office, along with the U.S. Department of Homeland Security Chief Privacy Officer, U.S. Citizenship and Immigration Services, and Science and Technology Silicon Valley Innovation Program representatives, presented at the 2024 Federal Privacy Council Summit. The session focused on delivering privacy-preserving digital credentials and provided an overview of Science and Technology efforts in this area.
  The Science and Technology Directorate Privacy Office, in collaboration with the Department of Homeland Security Privacy Office and representatives from the Cybersecurity and Infrastructure Security Agency, participated in a panel discussion at the U.S. Department of Homeland Security Silicon Valley Innovation Program's Synthetic Data Generator Industry Day. The panel focused on Department of Homeland Security use cases for privacy-preserving technical capabilities that generate and utilize synthetic data.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

- The Science and Technology Directorate Privacy Office conducted annual mandatory training for 50 staff members, covering essential privacy topics.
- The Science and Technology Directorate Privacy Office co-presented with Contract Acquisition Program Support, Security, and the Office of the Chief Information Officer for 200 staff members. The session focused on identifying and handling Controlled Unclassified Information, updates to key policies, and changes to the Homeland Security Acquisition Manual's Appendix G processes.

Transportation Security Administration

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

- The Transportation Security Administration Privacy Office conducted training for 70 Intelligence staff on First Amendment and Civil Liberties issues related to preparing Intelligence Products.
- The Transportation Security Administration Privacy Office conducted training for 93 Information System Security Officers on how to prepare a Privacy Threshold Analysis.

- The Transportation Security Administration Privacy Office conducted training for 49 reviewers on privacy considerations when processing reasonable accommodation requests.
- The Transportation Security Administration Privacy Office participated in the Biometric Identity Management Summit, which was attended by over 300 industry and privacy advocacy group representatives.
- The Transportation Security Administration Privacy Office conducted outreach to privacy advocacy groups on various topics, including the use of biometrics, Amtrak passenger assessment, and the use of watch lists.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

- The Transportation Security Administration Privacy Office provided five training sessions to 384 employees. These sessions covered topics ranging from basic privacy training and compliance requirements to advanced, role-specific topics, such as privacy, civil rights, and civil liberties considerations when conducting watch listing and law enforcement activities.
- The Transportation Security Administration Privacy Office participated in two briefings for external stakeholders on identification initiatives, including Real ID, biometrics, and digital ID.

U.S. Citizenship and Immigration Services

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

- The U.S. Citizenship and Immigration Services Privacy Office conducted Privacy Awareness training for 4,550 employees and contractors. This training provided annual reminders on privacy laws, policies, and requirements.
- The U.S. Citizenship and Immigration Services Privacy Office provided Privacy Awareness training for 350 new employees as part of the New Employee Orientation Program. This session equipped new hires with basic knowledge of privacy requirements and their responsibilities to safeguard personal information.
- The U.S. Citizenship and Immigration Services Privacy Office hosted monthly Drop-In Privacy Threshold Analysis training for 135 employees, focusing on providing a foundational understanding of how to complete a Privacy Threshold Analysis and its purpose.
- The U.S. Citizenship and Immigration Services Privacy Office conducted New Field Office Director Privacy Briefings for 15 directors. These briefings provided an overview of the privacy program and outlined the responsibilities of new directors and their leadership teams in promoting a culture of privacy.
- The U.S. Citizenship and Immigration Services Privacy Office disseminated Quarterly Privacy Tips focused on protecting personal information and best practices for safeguarding privacy.
- The U.S. Citizenship and Immigration Services Privacy Office launched and broadcasted the inaugural Office of Privacy spotlight as part of an initiative to raise awareness about different directorates and program offices. The first spotlight provided an overview of the Office of Privacy in conjunction with Annual Data Privacy Day on January 28, 2024.
- The U.S. Citizenship and Immigration Services Privacy Office provided specialized training to the Information Security Division Risk Management Branch on privacy compliance requirements for information technology systems. This training guided over 180 employees and contractors through the privacy compliance lifecycle, from the initial Privacy Threshold Analysis to system decommissioning and the need for a Disposition Privacy Threshold Analysis.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

- The U.S. Citizenship and Immigration Services Privacy Office presented Privacy and Information Sharing training to senior leadership of the Refugee, Asylum, and International Operations Directorate's International and Refugee Affairs Division at their Leadership Conference in Washington, D.C. The session provided an overview of the Office of Privacy, information sharing rules, processes, procedures, and privacy compliance information. Participants included leaders of international operations at various consulates worldwide, including the leadership of the two offices in China.
- The U.S. Citizenship and Immigration Services Privacy Office conducted bi-weekly instructor-led Privacy Awareness Training for 345 onboarding federal employees and contractors at headquarters.
- The U.S. Citizenship and Immigration Services Privacy Office conducted instructor-led training for 59 federal employees and contractors as part of the privacy segment of the Fundamentals of Mission Support Training.
- The U.S. Citizenship and Immigration Services Privacy Office conducted instructor-led training for 89 federal employees from the Fraud Detection and National Security division, who completed the Privacy Training for the Operational Use of Social Media.
- The U.S. Citizenship and Immigration Services Privacy Office reported that 21,786 federal employees and contractors completed the 2024 Privacy Awareness Training.
- The U.S. Citizenship and Immigration Services Regional Privacy Officers maintain an ongoing privacy outreach plan that includes sending out Monthly Broadcasts with Privacy Tips and Best Practices, as well as offering training opportunities for District Offices, Field Offices, and Asylum Offices. The plan also includes Monthly Privacy Touch Base meetings with leadership to discuss privacy concerns and new projects. This outreach ensures consistent communication and support for privacy awareness across the region.
- The U.S. Citizenship and Immigration Services Privacy Office conducted Monthly Western Region Drop-In Privacy Threshold Analysis Training for 73 attendees.
- The U.S. Citizenship and Immigration Services Privacy Office conducted a Regional Privacy Officer New Employee Orientation for 62 attendees.
- The U.S. Citizenship and Immigration Services Privacy Office conducted a Western Region Executive Briefing on Privacy Awareness for three attendees.
- The U.S. Citizenship and Immigration Services Privacy Office conducted International Officer's Basic Training on Information Sharing for 26 attendees.
- The U.S. Citizenship and Immigration Services Privacy Office conducted Field Office Director Privacy Awareness Training for 35 attendees.

U.S. Coast Guard

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

- The U.S. Coast Guard Privacy Office presented new employee privacy awareness training at 12 Civilian Employee Orientation sessions, attended by160 employees.
- The U.S. Coast Guard Privacy Office distributed flyers to all Commands investigating confirmed or suspected privacy incidents, providing instructions on encrypting electronic sensitive information.
- The U.S. Coast Guard Privacy Office composed three informational notices, which were broadcast on television screens throughout the St. Elizabeth Campus.
- The U.S. Coast Guard Privacy Office developed a Privacy Incident Standard Operating Procedure to guide the response and tracking of privacy incidents.

- The U.S. Coast Guard Privacy Office expanded its privacy awareness campaign beyond headquarters by publishing the following "Seasonal" Special Notices on the Coast Guard Portal Special Notices page:
    - Avoiding Tax-related Identity Theft
    - Be Privacy-Conscious During Transfer Season
    - Holiday Bustle: Be Aware – The Holiday Season Invites Criminal Activity

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

- The U.S. Coast Guard Privacy Office presented new employee privacy awareness training at 12 Civilian Employee Orientation sessions, attended by 150 employees.
- The U.S. Coast Guard Privacy Office expanded its privacy awareness campaign beyond headquarters by publishing the following "Seasonal" Special Notices on the Coast Guard Portal Special Notices page:
    - Tax-related Identity Theft: Don't Be a Victim!
    - Be Privacy-Conscious During Transfer Season

U.S. Customs and Border Protection

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

- The U.S. Customs and Border Protection Privacy Office provided instructor-led training to 419 personnel on privacy basics, compliance, and information sharing, helping to create a culture of privacy awareness within the agency. This training covered topics such as data protection, sharing requirements, and compliance, and was delivered virtually to various operational offices within the Office of Field Operations, Border Patrol, Office of International Affairs, and other essential program offices. The training sessions included Information Sharing (Domestic & Foreign), Foundational Privacy Awareness, Privacy Compliance, Operational Use of Social Media, and the application of the Federal Acquisition Regulation Security & Privacy clauses through the Homeland Security Acquisition Regulation and International Traffic in Arms Regulations procurement process.
- The U.S. Customs and Border Protection Privacy Office continued its training efforts in support of the Foreign Information Sharing and Domestic Information Sharing Directives for Law Enforcement and Security Purposes, with a particular emphasis on the Foreign Disclosure Directive. These trainings provided guidance on the processes and parameters for sharing records maintained by U.S. Customs and Border Protection with foreign and domestic law enforcement agencies/partners, allowing operational offices to process requests for information without requiring prior coordination with the Department of Homeland Security Privacy Office. Additionally, an abridged version of this training is available to all employees via the agency's Learning Management System.
- The U.S. Customs and Border Protection Privacy Office hosted an "Annual Lunch & Learn" training symposium with the Office of Acquisitions and partnered with subject matter experts from the Office of Acquisition on International Traffic in Arms Regulations and the Homeland Security Acquisition Regulation. These sessions focused on the application of Homeland Security Acquisition Regulation Class Deviation clauses in contracts, along with other privacy fundamentals. During the reporting period, the U.S. Customs and Border Protection Privacy Office reviewed 330 Homeland Security Acquisition Regulation and International Traffic in Arms Regulations submissions.
- The U.S. Customs and Border Protection Privacy Office deployed privacy awareness campaigns and messaging through the agency's "Information Display System," main internal webpage, and other information delivery channels, highlighting the importance of privacy awareness and responsibilities

under the Privacy Act of 1974. Messages were streamed monthly, including seasonal and holiday-themed content.

- The U.S. Customs and Border Protection Privacy Office reported that 25,304 personnel completed the mandatory annual computer-assisted privacy awareness training course, "Privacy at the Department of Homeland Security: Protecting Personal Information."
- The U.S. Customs and Border Protection Privacy Office reported that 419 personnel completed instructor-led privacy training courses.
- The U.S. Customs and Border Protection Privacy Office reported that 42,438 personnel completed the social media training course.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

- The U.S. Customs and Border Protection Privacy Office reported that 1,621 personnel completed the instructor-led privacy training course.
- The U.S. Customs and Border Protection Privacy Office reported that 75,121 personnel completed the mandatory annual computer-assisted privacy awareness training course, "Privacy at the Department of Homeland Security: Protecting Personal Information."
- The U.S. Customs and Border Protection Privacy Office reported that 57,423 personnel completed the Operational Use of Social Media course, as required by the U.S. Department of Homeland Security Directive Instruction Number 110-01-001, Privacy Policy for Operational Use of Social Media. Additionally, 1,251 personnel completed the Personal Use of Social Media course.
- The U.S. Customs and Border Protection Privacy Office provided instructor-led training in support of both the Foreign and Domestic Information Sharing Directives for Law Enforcement and Security Purposes. These sessions guided participants through the processes and parameters for sharing records owned by U.S. Customs and Border Protection with foreign and domestic law enforcement agencies, highlighting operational offices' ability to process information requests without requiring prior coordination with the U.S. Customs and Border Protection Privacy Office.
- The U.S. Customs and Border Protection Privacy Office developed, completed, and implemented an overarching online training program titled "Information Sharing for Employees," available via the agency's Learning Management System. This training outlines the processes for handling requests for information from foreign authorities and domestic agencies not covered by established Information Sharing Agreements and explains the discretionary sharing of information in accordance with relevant directives.
- The U.S. Customs and Border Protection Privacy Office hosted its "Annual Lunch & Learn" training symposium in collaboration with the Office of Acquisitions and continued to partner with subject matter experts on International Traffic in Arms Regulations and Homeland Security Acquisition Regulation training. These sessions facilitated discussions on the application of Homeland Security Acquisition Regulation Class Deviation clauses in contracts, and during the reporting period, the Privacy Office reviewed 581 submissions.
- The U.S. Customs and Border Protection Privacy Office continued deploying privacy awareness campaigns via the agency's "Information Display System," internal webpage, and other delivery channels, reinforcing the importance of privacy awareness and employee responsibilities under the Privacy Act of 1974.
- The U.S. Customs and Border Protection Privacy Office expanded its partnership with the Office of Information Technology – Cyber Defense Forensics Team to enhance the email blocking/encryption sensitivity label tool, which now includes Import and Trade-related personally identifiable information. Since the program's inception in June 2022, employees have applied encryption using the sensitivity label 1,387,140 times, and the tool has blocked 362,678 messages that would have otherwise violated policy.

U.S. Secret Service

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

- The U.S. Secret Service provided instructor-led privacy training to 86 personnel.
- The U.S. Secret Service reported that 568 personnel completed the mandatory annual computer-assisted privacy awareness training course.
- The U.S. Secret Service reported that 409 staff members completed the operational use of social media training.
- The U.S. Secret Service Privacy Program created a poster and fact sheet, posted an official message on the intranet, and displayed a digital version to commemorate Privacy Day.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

- The U.S. Secret Service provided instructor-led privacy training to 291 personnel.
- The U.S. Secret Service reported that 4,111 personnel completed the mandatory annual computer-assisted privacy awareness training course.
- The U.S. Secret Service reported that 525 staff members completed the operational use of social media training.
- The U.S. Secret Service provided privacy training for 442 new employees during this period.

PRIVACY COMPLAINTS

The U.S. Department of Homeland Security Privacy Office is responsible for ensuring that procedures are in place to receive, investigate, respond to, and provide redress for privacy complaints. Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*, as amended, requires the Department of Homeland Security Privacy Office 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.

The U.S. Department of Homeland Security 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. The U.S. Department of Homeland Security 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.

The U.S. Department of Homeland Security 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 Freedom of Information Act or Privacy Act requests) or correction to personally identifiable information held by the Department of Homeland Security. Redress also includes privacy-related complaints under the Department of Homeland Security Traveler Redress Inquiry Program. 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 U.S. Department of Homeland Security Privacy Office reviews redress complaints received by the Department's Traveler Redress Inquiry Program that may have a privacy nexus. The Traveler Redress Inquiry Program 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 Traveler Redress Inquiry Program 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.*

First Half of FY 2024 (October 1, 2023 – March 31, 2024)

During the first half of FY 2024, the Department received **144** privacy complaints outside of the Traveler Redress Inquiry Program process.

Type	CBP	CISA	FEMA	FPS	FLETC	ICE	TSA	USCIS	USCG	USSS	TOTAL
Procedure	1	0	0	0	0	0	38	0	0	0	**39**
Redress	0	0	0	0	0	0	0	0	0	0	**0**
Operational	6	0	0	0	0	0	99	0	0	0	**105**
Referred	0	0	0	0	0	0	0	0	0	0	**0**
TOTALS	**7**	**0**	**0**	**0**	**0**	**0**	**137**	**0**	**0**	**0**	**144**

Procedure and Operational Examples

- A U.S. citizen traveler with Global Entry authorization complained about delays with the inspection process by U.S. Customs and Border Protection after the arrival of a flight from Cuba. U.S. Customs and Border Protection provided the complainant with information regarding the traveler redress process.
- A U.S. citizen complained that during an encounter with the complainant's wife, a U.S. Customs and Border Protection Officer required the wife to provide the complainant's information and claimed to run it through U.S. Customs and Border Protection systems. The complainant alleges this is a privacy violation since the complainant was not involved in the encounter. U.S. Customs

and Border Protection provided the complainant with information regarding the traveler redress process.

- A complainant reported that he and his family have been unfairly delayed by U.S. Customs and Border Protection inspection processes despite having a U.S. Department of Homeland Security traveler redress number. He alleged that he is subjected to additional inspection because he previously complained that U.S. Customs and Border Protection was discriminatorily selecting subjects for additional inspection. U.S. Customs and Border Protection referred the complaint to the Office for Civil Rights and Civil Liberties.
- A U.S. citizen complained that U.S. Customs and Border Protection agents lost his passport during inspection at the Newark Airport. U.S. Customs and Border Protection provided the complainant with information on how to file a claim.
- A U.S. citizen complained that a U.S. Customs and Border Protection Officer abused his authority during an encounter and shared the complainant's personal information with other individuals in the inspection area. The Customs and Border Protection Field Office responded to the complaint.

Second Half of FY 2024 (April 1, 2024 – September 30, 2024)

During second half of FY 2024, the Department received **145** privacy complaints outside of the Traveler Redress Inquiry Program process.

Type	CBP	CISA	FEMA	FPS	FLETC	ICE	TSA	USCIS	USCG	USSS	CRCL	TOTAL
Procedure	0	0	0	0	0	2	8	0	0	0	10	**10**
Redress	0	0	0	0	0	47	0	0	0	0	0	**47**
Operational	4	0	0	0	0	26	56	0	0	0	0	**86**
Referred	0	0	0	0	0	2	0	0	0	0	0	**2**
TOTALS	**4**	**0**	**0**	**0**	**0**	**77**	**64**	**0**	**0**	**0**	**10**	**145**

Procedure and Operational Examples

- A complainant reported that they and their spouse were traveling through Aruba Preclearance. At primary inspection, the officer rudely told the spouse to come forward if they were traveling together and made belittling comments. The officer discovered the subject had a protection order and loudly asked about it, which others could hear. The supervisor apologized for the inappropriate questions about the protection order. The subject was referred to the Complaint Resolution Center and believes the officer needs training to be nicer.
- An individual was pulled for additional aviation security screening, during which an employee, accompanied by two non-officers, used the individual and their bags for training purposes. This was unprofessional and unauthorized, sharing personal information with non-officers. The individual's medical devices, including a knee brace and a Continuous Positive Airway Pressure machine, were unnecessarily handled. This incident resulted in the individual being late for their flight, causing pain due to medical conditions, and had to plead to board instead of being placed on standby. Missing a government-paid flight could result in serious administrative consequences, including job loss. The individual was used as a training aid and feels this violates their privacy.
- A traveler arrived at Miami Airport, went through immigration and was taken to secondary inspection. After waiting, she asked for help, and a female officer told her to wait due to an investigation. The traveler ended up losing her passport with the visa. The officer searched her luggage but couldn't find it and accused her of having it. She was released without explanation or a

document. Later, it was suggested that the passport was likely given to someone else by mistake. The traveler now faces costs to replace the passport and visa and seeks assistance to resolve the issue.

- The Immigration and Customs Enforcement Office of Professional Responsibility received information indicating the agency failed to provide Freedom of Information Act documentation to an Enforcement and Removal Operations employee regarding the selection and hiring process of a position. The matter was denoted as information only and the investigation was closed.
- The Immigration and Customs Enforcement Office of Professional Responsibility received information indicating mail addressed to an Immigration and Customs Enforcement detainee from his attorney and containing confidential asylum application information was released to another detainee with the same country of citizenship and same last name. The incident was reviewed by management and closed.
- The Immigration and Customs Enforcement Office of Professional Responsibility received a self-report from an Immigration and Customs Enforcement Homeland Security Investigations special agent who inadvertently downloaded or transferred child sexual abuse material and other explicit materials. The agent attempted to cancel the action but was unsuccessful. The matter was referred to the Office of Inspector General in accordance with the U.S. Department of Homeland Security Management Directive.
- The Immigration and Customs Enforcement Office of Professional Responsibility received information from an Immigration and Customs Enforcement Homeland Security Investigations group supervisor reporting an allegation that law enforcement personnel may have disclosed information concerning a targeted subject to a transnational criminal organization.
- A non-governmental organization alleges that Muslim community members have reported being asked or forced to have their photographs taken by federal agents at airports in Southern California. Clients have reported that once they completed security screening, an agent would take their picture with what seemed to be a personal phone. No other details were provided.
- The Office of Civil Rights and Civil Liberties received a submission about a government surveillance incident at Port Everglades Terminal, Ft. Lauderdale. The individual, escorted off the Holland America Rotterdam cruise ship for secondary inspection, was told by an officer his lost/stolen passport was revoked due to International Megan's Law, requiring a stamp for covered sex offenders. The individual explained the passport was revoked, and when applying for a new one, he marked it as lost/stolen since there was no option to indicate revocation. After two hours, an officer searched his bag and asked to unlock his phone, with the officer stating this likely wouldn't happen every time. The individual claims the incident caused anxiety for him and his wife. He explained he was convicted of Aggravated Criminal Sexual Abuse in 2010, is a lifetime registered sex offender in Illinois, and feels the ongoing surveillance is excessive and unjustified.
- The Office of Civil Rights and Civil Liberties received a submission from the National Immigration Justice Center on behalf of a Venezuelan asylum seeker, alleging U.S. Customs and Border Protection breached confidentiality by sharing her personal information with the Venezuelan embassy without consent. The individual, who protested the Venezuelan government, was previously detained and tortured by the Venezuelan National Guard. The submission includes U.S. Department of Homeland Security documentation alerting the embassy to her detention. The complainant claims U.S. Customs and Border Protection violated 28 CFR 50.5(a)(1), which requires informing detainees of their right to consular notification and argues U.S. Customs and Border Protection's actions put her at risk of further harm. The complainant urges the Office of Civil Rights and Civil Liberties to investigate a possible pattern of abuse by U.S. Customs and Border Protection.

- The Office of Civil Rights and Civil Liberties received a webform submission from the Florence Immigrant and Refugee Rights Project on behalf of an unaccompanied alien child, 12 years old, who was apprehended on July 10, 2024, near Santa Teresa, New Mexico. The child was processed at the El Paso Hardened Facility and was transported to the U.S. Department of Homeland Security Office of Refugee Resettlement on July 12, 2024. The child alleged she did not like that the female agents told her to "strip clothes" outside in front of the officers and to finish changing her clothes in their makeshift bathroom with a curtain. The child alleged they inspected all their clothes beforehand and there was no reason to have them take their clothes off in that manner.
- The Office of Civil Rights and Civil Liberties received direct correspondence from a complainant who alleged she was denied the ability to opt out of the facial recognition biometrics system at the San Francisco International Airport. The complainant alleged the officer pressured and intimidated her, stating that she could not opt out of the biometrics photo. The complainant alleged the officer asked another officer at the desk next to him if she was allowed to opt out, to which they looked at her in an unsure way and "still said no". The complainant is requesting compensation and that her photo that was taken be removed.
- The Office of Civil Rights and Civil Liberties received direct correspondence from a complainant reporting that a U.S. Department of Homeland Security employee and a bail bondsman at Washington & Gray Bail Bonds allegedly looked up her immigration status and provided it to another employee at Washington and Gray Bonds. The complainant alleged her privacy was breached.
- The Office of Civil Rights and Civil Liberties received an email in Spanish from a complainant, an individual in Immigration and Customs Enforcement custody at the T. Don Hutto Detention Center in Taylor, Texas, who had been at South Texas Immigration and Customs Enforcement Processing Center in Pearsall, Texas, when the alleged incident occurred. The complainant claimed that a data breach on November 28, 2022, exposed information about his credible fear case, putting his and his family's lives at risk.
- The Office of Civil Rights and Civil Liberties received an email from the attorney of an individual detained at Moshannon Valley Processing Center. The complainant alleges that NBC News aired his client's identity and asylum information, citing two U.S. Immigration and Customs Enforcement officials. He provided links to the episode and a similar NBC story. The complainant claims this violated his client's confidentiality rights (8 CFR Sec. 208.6), as his client never consented to the disclosure, and the ISIS ties label has endangered his safety.
- The Office of Civil Rights and Civil Liberties received a referral from the Office of Inspector General from an anonymous complainant alleging privacy violations at Krome North Service Processing Center. The complainant claims officers at the facility are not only searching for contraband but also scanning and copying detainees' personal information, including documents and letters from attorneys.
- A complainant alleged that U.S. Immigration and Customs Enforcement will not release his client's medical records without filing a Freedom of Information Act request. The Office of Civil Rights and Civil Liberties was copied on an email from the Brooklyn Defender Services directed to the Duty Officer and Deportation Officer on behalf of his client, an individual in U.S. Immigration and Customs Enforcement custody at the Buffalo Service Processing Center in Batavia, New York. The complainant alleged that his office has requested the noncitizen's medical records but was notified that the records could only be attained by filing a Freedom of Information Act request. The complainant attached a privacy waiver that he states permits U.S. Immigration and Customs Enforcement to transmit the noncitizen's medical records to him as the noncitizen's attorney, and there is no requirement that a Freedom of Information Act request must be submitted.

- The U.S. Citizenship and Immigration Services provided the U.S. Department of Homeland Security Privacy Office with justification for actions related to three recommendations from the U.S. Department of Homeland Security Privacy Compliance Review for Privacy Incidents Affecting Individuals Protected by Section 1367. The review involved U.S. Citizenship and Immigration Services, U.S. Customs and Border Protection, and U.S. Immigration and Customs Enforcement, which all have access to Section 1367 applicant information. U.S. Citizenship and Immigration Services addressed Recommendations 1, 2, and 3, including establishing a Section 1367 working group, publishing related policies, and updating technology to reduce bulk sharing with the Federal Bureau of Investigation. The U.S. Department of Homeland Security Privacy Office is reviewing U.S. Citizenship and Immigration Services responses to assess partial or full implementation of the recommendations

APPENDIX A– PUBLISHED PRIVACY IMPACT ASSESSMENTS

Privacy Impact Assessments Published October 1, 2023 March 31, 2024	
DHS Component and System Name	**Date Published**
DHS/CBP/PIA-014(b) Centralized Area Video Surveillance System	10/4/2023
DHS/USCIS/PIA-090 USCIS ArcGIS Enterprise System	10/15/2023
DHS/ALL/PIA-097 Use of Conditionally Approved Commercial Generative Artificial Intelligence Tools	11/19/2023
DHS/ICE/PIA-063 ICE Non-citizen Portal	11/20/2023
DHS/CBP/PIA-051(b) Mobile Passport Control	11/21/2023
DHS/TSA/PIA-046(d) TDC Automation Using Facial Identification	11/29/2023
DHS/ICE/PIA-064 ICE Operational Use of Publicly Available Information Including Social Media Information for Law Enforcement Investigations	12/15/2023
DHS/ALL/PIA-072 National Vetting Center	2/6/2024
DHS/ALL/PIA-084 Joint-Threat Information Management System (J-TIMS)	2/10/2024
DHS/S&T/PIA-031(a) Select Agent Inventory	2/26/2024
DHS/USCG/PIA-022(a) Coast Guard Maritime Information eXchange (CGMIX)	2/26/2024
DHS/CISA/PIA-035 National Cybersecurity Protection System (NCPS) - Core Infrastructure	3/5/2024
DHS/S&T/PIA-044 Cloud-based Biometric Analytic Environment (CBAE)	3/26/2024

Privacy Impact Assessments Published April 1, 2024 September 30, 2024	
DHS Component and System Name	**Date Published**
DHS/CBP/PIA-007(i) Electronic System for Travel Authorization (ESTA)	4/26/2024
DHS/USCIS/PIA-075(a) RAILS	5/3/2024
DHS/USSS/PIA-017(b) Forensics Service Division System	5/6/2024
DHS/OIG/PIA-004 OIG TeamMate	5/9/2024
DHS/CBP/PIA-007(j) Electronic System for Travel Authorization (ESTA)	7/12/2024
DHS/USSS/PIA-032 eForce (formerly known as Use of Force) Reporting Application System)	7/30/2024
DHS/FEMA/PIA-059 Individual Assistance Systems	8/13/2024
DHS/CBP/PIA-081 Criminal Case Management System - Cloud (CCMS)	8/15/2024
DHS/CBP/PIA-006(e) Automated Targeting System	8/26/2024
DHS/USSS/PIA-033 USSS Use of Facial Recognition Services	9/12/2024
DHS/FLETC/PIA-003(a) eFLETC	9/18/2024

APPENDIX B – PUBLISHED SYSTEM OF RECORD NOTICES

System of Record Notices Published April 1, 2024 September 30, 2024	
DHS Component and System Name	**Date Published**
DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records	7/5/2024
DHS/FEMA-008 Disaster Recovery Assistance Files System of Records	9/9/2024