



Department of Homeland Security

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

July 2024



Homeland
Security

I am pleased to present the *U.S. Department of Homeland Security Privacy Office Fiscal Year 2023 Second Semiannual Report to Congress*.¹

This report highlights the Department's work to safeguard privacy and enhance transparency while protecting the homeland. The DHS Privacy Office provides policy and programmatic oversight and supports privacy policy implementation across the Department. It undertakes these responsibilities in collaboration with DHS Component Privacy² and Freedom of Information Act (FOIA) Officers, privacy points of contact, and program offices to implement privacy safeguards and enhance transparency across DHS.

This report provides details regarding privacy compliance documentation published during the reporting period, and the Privacy Office's advice and the response to its advice. Additionally, this report highlights Component privacy initiatives and privacy complaints received.

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
Chair, 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

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 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>.

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

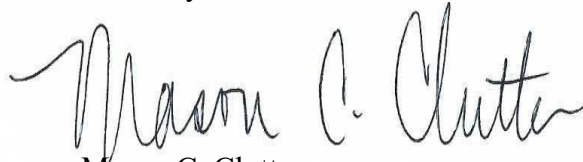
The Honorable Jerrold Nadler
Ranking Member, House Committee on the Judiciary

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

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

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,

A handwritten signature in black ink that reads "Mason C. Clutter". The signature is written in a cursive style with a large initial 'M' and 'C'.

Mason C. Clutter
Chief Privacy Officer and Chief FOIA Officer
U.S. Department of Homeland Security



DHS Privacy Office

April 1, 2023, to September 30, 2023

Semiannual Report to Congress

Table of Contents

LEGISLATIVE LANGUAGE.....	5
BACKGROUND	6
PRIVACY REVIEWS.....	8
Privacy Impact Assessments.....	10
System of Records Notices.....	13
ADVICE AND RESPONSES.....	14
Privacy Compliance Reviews	14
COMPONENT PRIVACY AWARENESS INITIATIVES.....	14
Cybersecurity and Infrastructure Security Agency (CISA)	14
Federal Emergency Management Agency (FEMA)	14
Science and Technology Directorate (S&T).....	15
Transportation Security Administration (TSA).....	15
U.S. Citizenship and Immigration Services (USCIS)	15
U.S. Coast Guard (USCG).....	16
U.S. Customs and Border Protection (CBP)	16
U.S. Secret Service (USSS).....	17
PRIVACY COMPLAINTS	18
APPENDIX A– PUBLISHED PRIVACY IMPACT ASSESSMENTS	20

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).

BACKGROUND

The DHS Chief Privacy Officer is the first statutorily mandated Chief Privacy Officer in the federal government. Section 222 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 Privacy Office collaborates with Privacy Officers,⁴ Privacy Points of Contact (PPOC),⁵ and program offices on the development of privacy policy and preparation of privacy compliance documentation.

DHS Privacy Office	Component Privacy Officers	Privacy Points of Contact
<ul style="list-style-type: none"> • Privacy Policy and Oversight Team • Privacy Compliance Team 	<ul style="list-style-type: none"> • 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) • U.S. Coast Guard (USCG) • U.S. Customs and Border Protection (CBP) • U.S. Immigration and Customs Enforcement (ICE) • U.S. Secret Service (USSS) 	<ul style="list-style-type: none"> • 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 Situational Awareness (OSA) • Office of Public Affairs (OPA) • Office of the Chief Security Officer (CSO) • Office of Homeland Security Statistics (OHSS)

⁴ DHS policy requires every DHS 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>.

⁵ 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 DHS Privacy Office to manage privacy matters within DHS.

DHS Privacy Office	Component Privacy Officers	Privacy Points of Contact
	<ul style="list-style-type: none"> • 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

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 privacy impact. 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*,⁶ the *Homeland Security Act of 2002*,⁷ 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.⁸
4. Privacy Act Statements, as required under the Privacy Act,⁹ 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*.¹⁰
6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*.¹¹
7. Privacy Compliance Reviews, per the authority granted to the Chief Privacy Officer by the Homeland Security Act of 2002.¹²
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.¹³
10. Other privacy reviews at the discretion of the Chief Privacy Officer.

⁶ 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.

⁷ 6 U.S.C. § 142.

⁸ 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>.

⁹ 5 U.S.C. § 552a(e)(3).

¹⁰ 5 U.S.C. § 552a(o)-(u).

¹¹ 42 U.S.C. § 2000ee-3.

¹² 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.

¹³ 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 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:	
<i>Type of Review</i>	<i>Number of Reviews</i>
	2nd Half of FY 2023 <i>April 1, 2023 – September 30, 2023</i>
Privacy Threshold Analyses	1,225
Privacy Impact Assessments	15
System of Records Notices and associated Privacy Act Exemptions	0
Privacy Act (e)(3) Statements ¹⁴	210
Computer Matching Agreements ¹⁵	2
Data Mining Reports	0
Privacy Compliance Reviews	0
Privacy Reviews of IT and Program Budget Requests ¹⁶	50
Information Technology Acquisition Reviews ¹⁷ (ITAR)	475
Other Privacy Reviews	0
<i>Total Reviews</i>	<i>1,977</i>

¹⁴ This total does not include all Components; several are permitted by the DHS Privacy Office to review and approve their own Privacy Act statements.

¹⁵ Computer Matching Agreements are typically renewed or re-established.

¹⁶ 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.

¹⁷ 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 include appropriate privacy safeguards. In addition to completing privacy impact assessments for new systems, projects, programs, pilots, or information-sharing arrangements that impact privacy, the Department also conducts triennial reviews of existing privacy impact assessments to evaluate and confirm systems' operation within original parameters and to implement additional safeguards as needed. After the triennial review, the Department updates and publishes a revised privacy impact assessment for the respective program, system, or activity if appropriate.

As of September 30, 2023, 100 percent of the Department's Federal Information Security Modernization Act systems requiring a privacy impact assessment had a current privacy impact assessment.

All published DHS privacy impact assessments are available on the DHS Privacy Office website, www.dhs.gov/privacy.¹⁸

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 in the Appendix.

New Privacy Impact Assessments

[DHS/TSA/PIA-053 TSA Unmanned Aircraft Systems](#) (April 24, 2023)

TSA is responsible for security for all modes of public transportation and has broad authority to assess security threats to the transportation sector and to direct implementation of measures intended to safeguard security at airports and other transportation facilities. Among its programs, TSA conducts vulnerability assessments at airports and other transportation centers and plans to operate unmanned aircraft systems (UAS) to improve these assessments. TSA may also use UAS for law enforcement operations at special events and to assist with the response to transportation incidents such as rail accidents, pipeline spills, or downed aircraft.

[DHS/FEMA/PIA-058 Hermit's Peak/Calf Canyon Claims and Loss Information Portal \(CLIP\)](#) (April 27, 2023)

FEMA, Office of Response and Recovery (ORR) Hermit's Peak/Calf Canyon Claims Office Program uses the Hermit's Peak/Calf Canyon Claims and Loss Information Portal to manage claims associated with the Hermit's Peak/Calf Canyon Fire. The system is designed to streamline and support the claims process to ensure accurate and timely execution of claims to compensate victims of the fire.

[DHS/USCIS/PIA-088 Fugitives and Absconders Search Report \(FASR\)](#) (May 22, 2023)

USCIS developed the Fugitives and Absconders Search Report (FASR) to support the reporting of absconders. As part of the background check process conducted when an applicant files an immigration request, USCIS identifies absconders and reports that information to ICE.

¹⁸ 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.

[DHS/TSA/PIA-054 Security Threat Assessments of Certain Surface Transportation Employees](#) *(July 13, 2023)*

TSA proposed a regulation to carry out the provisions of the Implementing Recommendations of the 9/11 Commission Act of 2007, which requires TSA to conduct security threat assessments of frontline public transportation, railroad employees, and security coordinators for those entities and over-the-road-bus operators. The proposed regulation would require certain employees to submit personal information to TSA to conduct security threat assessments.

[DHS/USSS/PIA-031 USSS Incident Driven Video Recording System \(IDVRS\)](#) *(July 21, 2023)*

USSS is deploying Incident Driven Video Recording System (IDVRS) technology that provides enhanced transparency during recorded interactions between officers, special agents, and the public. In conformity with the Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, and to ensure the smooth implementation of a full IDVRS program across the agency, the Secret Service proposes to develop and deploy IDVRS technology amongst its diverse workforce of Uniformed Division personnel, special agents, and technical law enforcement personnel through a multi-year phased plan. IDVRS further allows personnel to safely perform their duties during encounters with the public, while also assisting in the collection of evidence for use in prosecutions. USSS conducted this Privacy Impact Assessment to assess the privacy risks associated with operational use of incident driven recording technology used during law enforcement interactions with the public, while also outlining the Service's intentions regarding footage retention and storage of information collected. This Privacy Impact Assessment discusses testing and evaluation pending funding, and future deployment, and will be updated prior to formal and final deployment.

[DHS/USCIS/PIA-089 USCIS Outreach and Engagement Program](#) *(September 8, 2023)*

USCIS conducts outreach and engagement activities aimed at individuals who have applied for immigration benefits through traditional outreach measures such as emails, text messages, third party outreach service providers (e.g., GovDelivery.com), and postcard mailings. USCIS plans to enhance and expand these activities to include outreach through online filing and accounts and web-based tools. This PIA discusses how USCIS outreach activities may use personally identifiable information (PII) from members of the public.

Updated Privacy Impact Assessments

[DHS/ICE/PIA-038\(a\) Data Analysis & Research for Trade Transparency System](#) *(April 11, 2023)*

Homeland Security Investigations (HSI) deployed an information system called the Data Analysis & Research for Trade Transparency System (DARTTS), which is a component system of HSI's larger Repository for Analytics in a Virtualized Environment (RAVEN) platform. DARTTS analyzes trade data to identify statistically anomalous transactions that may warrant investigation for money laundering or other import-export crimes. This system replaces a similar system previously in use by HSI, called FALCON-DARTTS, which had the same purpose and functionalities. This Privacy Impact Assessment update provides public notice of the existence of DARTTS within RAVEN and that the legacy FALCON-DARTTS system was retired.

[DHS/TSA/PIA-050\(a\) Amtrak Rail Passenger Threat Assessment](#) *(April 11, 2023)*

TSA is responsible for security in all modes of public transportation, including surface modes such as rail. Amtrak is a national passenger rail operator managing more than 300 trains a day to more than 500

destinations in the United States and Canada. TSA assessed, from an operational risk perspective, historical passenger data for travel within the Northeast corridor for several months beginning at the end of 2021, to determine the extent to which known or suspected terrorists may have traveled on Amtrak trains and to assess whether watchlist matching should be considered as a rail security enhancement. To conduct the assessment, Amtrak provided TSA with rail passenger personally identifiable information (PII) for TSA to match against the Terrorist Screening Dataset, commonly known as the “watchlist.” TSA now intends to assess passenger travel data on additional Amtrak rail routes and updated this Privacy Impact Assessment to reflect all approved Amtrak rail routes for assessment.

[DHS/ALL/PIA-072 National Vetting Center \(NVC\)](#) *(April 11, 2023)*

The NVC coordinates agency vetting efforts to locate and use relevant intelligence and law enforcement information to identify individuals who may present a threat to the homeland. Vetting Support Agencies electronically transmit relevant and appropriate information (Vetting Support Responses) to Adjudicating Agencies using NVC technology. The Vetting Support Responses include links or pointers to information that Vetting Support Agencies assess are valid and analytically significant identity matches. These links or pointers allow Analysts to view related information in other (typically classified) systems to which the Analyst has authorized access. Originally, the Vetting Support Responses only included these links or pointers, which meant that Analysts had to search other systems to access additional information. Now, Vetting Support Agencies may also provide relevant information from the Vetting Support Request that matches information in Vetting Support Agency holdings. Unlike the links or pointers information, this matched information is presented for Analysts to view in the NVC technology; however, Analysts will still need to access other systems outside of the NVC technology to view all relevant information from Vetting Support Agency holdings.

[DHS/CBP/PIA-033\(a\) Electronic Visa Update System \(EVUS\)](#) *(May 18, 2023)*

CBP Electronic Visa Update System (EVUS) is a web-based enrollment system that collects new and updated information from certain nonimmigrant non-citizens in advance of their travel to the United States. Enrolling with EVUS is a requirement for certain individuals traveling to the United States for temporary business or tourism using certain visa types. CBP published this Privacy Impact Assessment update to provide notice and to assess the privacy risks associated with recent modifications to the EVUS application questionnaire, including the addition of an optional social media field on EVUS applications.

[DHS/OIG/PIA-001\(c\) OIG Enforcement Data System \(EDS\)](#) *(May 25, 2023)*

The OIG maintains complaint and investigation-related files within the Enforcement Data System (EDS). EDS is the official OIG electronic case management system for investigations. The OIG Office of Investigations, Office of Counsel, and the Whistleblower Protection Unit use EDS to manage information relating to complaints and investigations of alleged criminal, civil, or administrative violations by DHS employees, contractors, grantees, beneficiaries, and other individuals and entities associated with DHS. EDS also tracks resources used in investigative activities. This Privacy Impact Assessment update documents several enhancements to the system.

[DHS/CISA/PIA-020\(c\) State, Local, Tribal and Private Sector Clearance Program for Critical Infrastructure](#) *(August 28, 2023)*

CISA updated the Private Sector Clearance Program for Critical Infrastructure’s Privacy Impact Assessment to account for the organizational changes that have taken place in the administration of the program at CISA. This update outlines changes to the program clearance process and to DHS Form

9014, *State, Local, Tribal and Private Sector Clearance Request Form* since the publication of the Privacy Impact Assessment Update in April 2018.

[DHS/TSA/PIA-033\(a\) TSA Enterprise Search Portal](#) (August 29, 2023)

TSA implemented an Enterprise Search Portal search capability to enable authorized users to search or discover data across separate TSA databases with a single search. TSA updated this Privacy Impact Assessment to reflect that the system (now known as the Real-time Analytic Platform for Incident Deterrence (RAPID)) will expand its search capability beyond the original three TSA databases. The intent of RAPID, as with the Enterprise Search Portal, is to provide greater efficiency and visibility into the data currently held by TSA in disparate databases.

[DHS/CBP/PIA-076\(a\) Collection of Advance Information from Certain Undocumented Individuals on the Land Border: Post Title 42](#) (September 19, 2023)

The CBP One mobile application allows certain undocumented individuals to submit biographic and biometric information to CBP in advance of their arrival in the United States, and to schedule a time to present themselves at a port of entry for processing. CBP conducted this Privacy Impact Assessment update to provide transparency regarding changes to the process because of the termination of Title 42, including a change to the way in which undocumented individuals schedule their arrival at a U.S. port of entry. CBP initially published this Privacy Impact Assessment update on May 12, 2023, to document changes occurring after the expiration of the public health emergency and Title 42. CBP revised and republished this Privacy Impact Assessment update in September 2023 to update the scheduling process.

[DHS/USSS/PIA-028\(a\) United States Secret Service Unmanned Aircraft Systems Program \(UAS\)](#) (September 27, 2023)

USSS employs small UAS (sUAS) for surveillance and law enforcement purposes in support of its protective and investigative mission. sUAS identify threats, mitigate vulnerabilities, and create secure environments for protected people, places, and events and further support Agency investigations into crimes against U.S. financial systems committed by criminals around the world and in cyberspace. sUAS-platformed video technology assists the Agency with securing protective sites/interests and further allows surveillance for law enforcement investigations or tactical operations. USSS updated this Privacy Impact Assessment to provide notice of its expanded use of sUAS for investigative purposes not addressed in the original Privacy Impact Assessment, and to assess the privacy impacts of using this technology for that purpose.

System of Records Notices

The Department publishes System of Records Notices consistent with requirements outlined in the *Privacy Act of 1974*, as amended.¹⁹ 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 OMB and Congress.

As of September 30, 2023, 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*. The Privacy Office did not publish new or updated System of Records Notices during the reporting period.

¹⁹ 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>.

ADVICE AND RESPONSES

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

Privacy Compliance Reviews

The Privacy Office conducts Privacy Compliance Reviews, pursuant to DHS policy, in collaboration with Component Privacy Officers or Privacy Points of Contact and the manager of the system or program being reviewed. These reviews study the system or program's compliance with privacy laws, regulations, and Departmental privacy policies. Through Privacy Compliance Reviews, the Privacy Office develops recommendations and then works with the Component Privacy Officers or Privacy Points of Contact to bring the system or program into compliance as necessary or identifies best practices to further protect privacy. Since 2010, the Privacy Office has made about 130 recommendations through the Privacy Compliance Review process. The Privacy Office has closed more than 110 of these recommendations.

COMPONENT PRIVACY AWARENESS INITIATIVES

Cybersecurity and Infrastructure Security Agency (CISA)

- On July 11 and 25, 2023, the CISA Office of Privacy, Access, Civil Liberties, and Transparency organized the CISA Privacy Incident Awareness & Response Training. Privacy analysts conducted a privacy training for all CISA employees to review how to identify a privacy incident and the incident reporting process. The training also covered a review of best practices for safeguarding personally identifiable information during working hours while teleworking or at the office.
- On September 15, 2023, the CISA Office of Privacy, Access, Civil Liberties, and Transparency briefed employees from CISA Intelligence on privacy, civil rights, and civil liberties requirements in intelligence analysis and production. This briefing included the criteria that require a pre-publication review of finished intelligence products, as well as a broad review of oversight requirements.
- CISA reported 5,968 employees completed the mandatory annual computer-assisted privacy awareness training course.
- The CISA Office of Privacy, Access, Civil Liberties, and Transparency provided a privacy briefing during New Employee Orientation for 450 new employees.
- CISA reported 12 employees completed Privacy Requirements for Operational Use of Social Media.
- The CISA Office of Privacy, Access, Civil Liberties, and Transparency produced two issues (April and July) of the quarterly privacy newsletter. The newsletter is distributed CISA-wide and posted on the CISA Office of Chief Privacy Officer internal intranet page.

Federal Emergency Management Agency (FEMA)

- FEMA Office of Chief Council, Information Law Branch conducted an annual training event for over 100 FEMA attorneys that focused on the legal requirements in compliance and litigation of the Privacy Act.
- FEMA Privacy conducted a training event for over 50 System Owners within FEMA to review the requirements of System Owners under the Privacy Act, E-Government Act, and DHS/FEMA policy.

Federal Protective Service (FPS)

- FPS Privacy and the Freedom of Information Office provided monthly privacy awareness briefings at the New Employee Orientation onboarding sessions. The training provided 82 new employees with the privacy compliance and oversight process at FPS and DHS.
- FPS Privacy and the Freedom of Information Office conducted a refresher training session for FPS Human Capital Management (HCM) to reinforce the basic privacy requirements for FPS personnel. The training reminded over 40 employees and contractors of their responsibility to handle personally identifiable information in accordance with laws, regulations, and policies to prevent privacy incidents within HCM.
- FPS Privacy and the Freedom of Information Office held weekly Privacy Act and Freedom of Information Act (FOIA) “train-the-trainer” deep-dive sessions for four internal staff members. The sessions were designed to enhance the skills of supporting staff in FPS Privacy and OGC so they can share their knowledge within the component’s divisions. The plan is to hold kick-off meetings to be able to answer questions and ensure privacy compliance documentation is completed on numerous projects.
- FPS Privacy and the Freedom of Information Office developed and provided role-based Privileged User Information Access Briefings to regional FPS officers and a limited number of U.S. Department of Justice, Drug Enforcement Agency (DEA) officers (~12) who received access to the FPS Region 9 Video Surveillance System (VSS) video-screening rooms.

Science and Technology Directorate (S&T)

- The S&T Privacy Officer and Deputy Privacy Officer conducted a brown bag event highlighting privacy compliance documentation requirements. The training was Directorate-wide and there were 133 employees in attendance.
- S&T provided training on all functions of the S&T Privacy Program to support the onboarding of the new S&T Chief of Staff and incumbent Deputy Chief of Staff.

Transportation Security Administration (TSA)

- TSA conducted calls with several advocacy groups and think tanks regarding many of TSA’s privacy programs. Topics of discussion included TSA’s biometric programs, watchlisting, mobile driver’s license implementation, and Amtrak rail passenger assessment.
- The TSA Privacy Officer was a panel speaker during an external stakeholder’s seminar series. During the program, he discussed TSA programs, privacy protections, and responded to questions from attendees.
- TSA engaged with the Privacy and Civil Liberties Oversight Board (PCLOB) to support its oversight review of TSA’s use of facial recognition at airports.
- TSA conducted training for 136 Information System Security Officers regarding Privacy Threshold Assessment requirements and common privacy issues.

U.S. Citizenship and Immigration Services (USCIS)

- USCIS Office of Privacy provided numerous training sessions for USCIS stakeholders on how to complete privacy compliance documentation, including multiple specialized trainings on the

development of Privacy Threshold Analyses for system development teams, project teams, and information system security officers across Program Offices and Directorates.

- USCIS Office of Privacy provided a presentation at the Los Angeles Verification Operation Center's Fall All Hands meeting to introduce the Privacy Office, give an overview of DHS privacy policies and the compliance process, and highlight best practices on protecting personally identifiable information when working from home.
- USCIS Office of Privacy conducted several training sessions to provide USCIS employees and contractors with the basic knowledge of privacy requirements and educate employees on their responsibilities to handle personal information in accordance with laws, regulations, and policies.
- USCIS Office of Privacy conducted a bi-weekly privacy awareness training for onboarding USCIS Headquarters employees.
- USCIS Office of Privacy provided instructor-led privacy training and awareness sessions for Fraud Detection and National Security (FDNS) personnel in support of Social Media Program activities.
- USCIS Office of Privacy conducted training for Contracting Officers and Contracting Officer's Representatives on how contracts are reviewed for privacy requirements and privacy risks associated with handling USCIS information are identified and mitigated.
- USCIS Office of Privacy provided instructor-led training for the privacy segment of the Fundamentals of Mission Support Training.
- USCIS Office of Privacy provided several ad hoc Privacy Threshold Analysis (PTA) training sessions to program managers, forms owners, and information collection specialists over this reporting period. The training provided nuanced guidance to assist these individuals in completing PTAs that ultimately required minimal (if any) edits from the USCIS Office of Privacy prior to DHS submission and adjudication.

U.S. Coast Guard (USCG)

- USCG Privacy presented new employee privacy awareness training at six bi-monthly USCG Civilian Employee Orientation sessions, which were attended by 170 employees.
- USCG reported 46 employees completed operational use of social media training.
- USCG reported that 21,160 personnel and contractors completed the mandatory annual computer-assisted privacy awareness training course during the reporting period.
- USCG continued providing flyers to all Commands investigating confirmed or suspected privacy incidents that contained information about the requirements and instructions for encrypting electronic sensitive information.
- USCG attended and provided privacy awareness information to all attendees of the 2023 Centralized Annual Training at CG Headquarters/Base National Capital Region, which is an event that provides the leadership of CG-6, Headquarters C5I offices, the C5I Service Center, Atlantic and Pacific Area Information Technology staffs, District IT Staffs, Base C5I Departments, and other CG C5I stakeholders with critical updates to key information, process changes, and organizational changes, with the goal of enhancing collaboration among the CG C5I Community.
- A USCG Privacy Analyst routinely attended the Assistant Commandant for C4IT (CG-6) Leadership and Diversity Advisory Council's (LDAC) monthly meeting and advised the Council on DHS / USCG policy for safeguarding personally identifiable information collected during LDAC activities and included information regarding privacy compliance reviews.

U.S. Customs and Border Protection (CBP)

- CBP Privacy Office reported that 1,152 personnel completed instructor-led privacy training.

- CBP Privacy Office reported that 54,670 personnel completed the mandatory annual computer-assisted privacy awareness training course during the reporting period.
- CBP Privacy Office reported that 16,712 personnel completed operational use of social media training.
- CBP Privacy Office provided training on “Domestic Information Sharing for Law Enforcement and Security Purposes.” This training was offered for all CBP personnel within the Office of Field Operations, U.S. Border Patrol, and Air & Marine Operations who routinely share information with CBP federal, state, and local law enforcement/security partners in support of the Domestic Information Sharing Directive (4320-033: Sharing Information for Law Enforcement and Security Purposes). The training helps to provide instruction explaining the processes and parameters around the sharing of records owned by CBP with domestic law enforcement partners, which allows operational offices to process requests for information without requiring specific prior coordination with the CBP Privacy Office. CBP Privacy also developed an abridged training available to all employees via the agency’s Learning Management System.
- CBP Privacy Office continues to advance the development of Sharing of Information with Foreign Authorities training, which will support the recently updated Directive on Foreign Disclosures (4320-025B).
- CBP Privacy Office provided virtual instructor-led training to various operational offices within the Office of Field Operations, Border Patrol, and other essential program offices. Courses provided include Foundational Privacy Awareness Training, Information Sharing Training (Domestic & Foreign), Privacy Compliance Training, and Social Media Training.
- CBP Privacy Office capitalized on its close partnership with the Office of Information Technology – Cyber Defense Forensics Team through collaboration efforts, which for the reporting period involved the expansion of the email blocking/encryption sensitivity label tool to include Import and Trade-related personally identifiable information. During the reporting period, employees applied encryption using the sensitivity label 339,364 times and the tool blocked 155,037 messages that would have otherwise resulted in a policy violation.
- CBP Privacy Office reviewed several hundred contracts as part of the established Privacy Compliance process. This coordination with the Office of Acquisitions has led to standing participation in an “Annual Lunch & Learn” training venue, designed to facilitate discussions of privacy inclusion in contract administration, with respect to Homeland Security Acquisition Regulation Class Deviation clauses and other privacy fundamentals.
- CBP Privacy Office continued to bolster and heighten personnel privacy awareness and responsibilities throughout the agency by broadcasting privacy messaging through 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. Secret Service (USSS)

- USSS trained 362 new employees virtually on privacy during New Employee Orientation.
- USSS provided instructor-led privacy training courses for 165 personnel.
- USSS reported 3,529 staff members completed operational use of social media training.
- USSS reported 6,136 personnel completed the mandatory annual computer-assisted privacy awareness training course.
- On August 24, 2023, the USSS Privacy Program sent an official message to all USSS employees reminding them of the Privacy Compliance Requirements. The official message described the privacy compliance process and what is expected in accordance with IGL-04, USSS Privacy Compliance Policy.

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. **Procedural:** 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 the 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 personally identifiable information 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 that 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 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 experienced during travel screening at transportation hubs, like airports or when crossing U.S. borders. This includes potential watchlist issues, screening at ports of entry, and situations in which 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, 95 travelers marked that box. Upon review, three of the complaints received through TRIP described a privacy violation.

During the reporting period, the Department received 75 privacy complaints outside of the TRIP process.

Type	CBP	CISA	FEMA	FPS	FLETC	ICE	TSA	USCIS	USCG	USSS	TOTAL
<i>Procedural</i>	3	0	0	0	0	0	15	0	0	0	18
<i>Redress</i>	0	0	0	0	0	0	0	0	0	0	0
<i>Operational</i>	8	0	0	0	0	2	47	0	0	0	57
<i>Referred</i>	0	0	0	0	0	0	0	0	0	0	0
TOTALS	11	0	0	0	0	2	62	0	0	0	75

Procedural and Operational Examples

- CBP Privacy Office received notification of a complaint from an individual that they are being targeted by CBP. The individual stated they are frequently asked if they work in Mexico and what they do for a living. The individual also stated that the officers repeatedly asked if they had any weapons or drugs.
- CBP Privacy Office received notification of a complaint that an employee is sharing sensitive data with family and friends and using information from agency files for personal dealings.
- CBP Privacy Office received notification from an individual that they may have received a spam email and that their Global Entry number had been accessed by another person.
- CBP Privacy Office received notification from an individual that their Green Card was lost by ICE. The individual was instructed by a supervisor to order a replacement. The individual applied for a replacement Green Card and is waiting to receive it.
- CBP Privacy Office received notification of a complaint that a person’s facial recognition scan and fingerprints were taken and incorrectly placed under a fellow traveler’s passport information/profile. According to the complainant, an officer told the person that the fingerprint scan could not be removed from the fellow traveler’s profile, but that a note was placed in the system explaining that the individual and the fellow traveler’s information had been “crossed.”
- ICE Privacy Unit received notification of a complaint related to the DHS Rideshare Program. An ICE employee received notice that HSI had enrolled the individual to participate in the Uber Rideshare Program after submitting a request to opt out.
- A passenger complained that TSA had violated their privacy rights by collecting facial biometrics at a security checkpoint without providing any notification or signage that the collection was optional. The airport had posted signage, but the passenger had missed seeing it while in line. TSA concluded that the signage could be improved, including changes to font size/coloring, overall simplification/reduction of the language, and relocation of the most important language (opt-out clause) to be upfront and bolded.

APPENDIX A– PUBLISHED PRIVACY IMPACT ASSESSMENTS

Privacy Impact Assessments Published April 1, 2023 – September 30, 2023	
DHS Component and System Name	Date Published
DHS/ICE/PIA-038(a) Data Analysis & Research for Trade Transparency System DARTTS	4/11/2023
DHS/TSA/PIA-050 Amtrak Rail Passenger Threat Assessment	4/11/2023
DHS/ALL/PIA-072 National Vetting Center	4/13/2023
DHS/TSA/PIA-053 TSA Unmanned Aircraft Systems	4/25/2023
DHS/FEMA/PIA-058 Hermit’s Peak/Calf Canyon Claims and Loss Information Portal (CLIP)	4/27/2023
DHS/CBP/PIA-033 Electronic Visa Update System	5/10/2023
DHS/CBP/PIA-076(a) Collection of Advance Information from Certain Undocumented Individuals on the Land Border: Post Title 42	5/12/2023
DHS/USCIS/PIA-088 Fugitives and Absconders Search Report	5/23/2023
DHS/OIG/PIA-001(c) Enforcement Data System	5/25/2023
DHS/TSA/PIA-054 Security Threat Assessments of Certain Surface Transportation Employees	7/13/2023
DHS/USSS/PIA-031 Incident Driven Video Recording System	7/21/2023
DHS/CISA/PIA-020(c) Private Sector Clearance Program for Critical Infrastructure	8/28/2023
DHS/TSA/PIA-033(a) Enterprise Search Portal	8/29/2023
DHS/USCIS/PIA-089 USCIS Outreach and Engagement Program	9/8/2023
DHS/USSS/PIA-028(a) Unmanned Aircraft Systems	9/27/2023