Department of Homeland Security

Privacy Office Semi-Annual Reports to Congress Covering October 2021 – March 2023

February 7, 2024

Homeland Security

February 7, 2024

I am pleased to present the *U.S. Department of Homeland Security Privacy Office Fiscal Year 2021 Second Semiannual Report to Congress.*[1] To return the Department to a regular reporting cadence and provide transparency into operations, this report covers three reporting periods:

- October 1, 2021 – March 31, 2022;
- April 1, 2022 – September 31, 2022; and
- October 1, 2022 – March 2023.

This report summarizes 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 Privacy[2] and Freedom of Information Act Officers, Privacy Points of Contact, and program offices to implement privacy safeguards and enhance transparency across DHS.

In addition to providing details regarding privacy compliance, this report highlights the Privacy Office's advice and the response to its advice. This report also includes updates to the Department's Privacy Compliance Review process. The Privacy Compliance Review process is a collaborative effort to assess a program's compliance with privacy requirements including requirements established in Privacy Impact Assessments and System of Records Notices, formal agreements such as Memoranda of Understanding, Memoranda of Agreements, and recommendations from the Chief Privacy Officer. A Privacy Compliance Review may result in a public report or internal recommendations, depending on the sensitivity of the program under review.

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,

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

[1] Pursuant to the Intelligence Authorization Act for Fiscal Year 2014, Pub. L. No. 113-126 (July 7, 2014), the reporting period was changed from quarterly to semiannually. 42 U.S.C. § 2000ee-1 (2014), Pub. L. No. 113-126, Title III, § 329(b)(4), 128 Stat. 1406 (2014). The DHS Privacy Office semiannual reports cover the following periods: April – September and October – March.

[2] DHS Components have a Privacy Officer and other DHS offices have a Privacy Point of Contact. A complete list can be found here: http://www.dhs.gov/privacy-office-contacts.

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

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

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

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

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

The Honorable Mark Warner
Chairman, Senate Select Committee on Intelligence

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

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

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

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

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

The Honorable Jim Jordan
Chairman, House Committee on the Judiciary

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

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

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

DHS Privacy Office
October 1, 2021- March 31, 2023
Semiannual Reports to Congress

Table of Contents

LEGISLATIVE LANGUAGE

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

"(f) Periodic Reports-

(1) In General –

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

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

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

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

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

(2) Contents – initiated

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 support the Department's 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
• 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 (Secret Service)	• 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 Immigration Statistics (OIS)

[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
	• Office of Biometric Identity Management (OBIM) • Office of Inspector General (OIG) • Federal Law Enforcement Training Centers (FLETC) • National Vetting Center (NVC) • Federal Protective Services (FPS)	

PRIVACY REVIEWS

The DHS Privacy Office reviews and evaluates Department programs, systems, and initiatives that collect personally identifiable information or otherwise have a privacy impact and provides mitigation strategies to reduce the 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 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.
8. Information Technology Acquisition Reviews.[12]
9. 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] 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.

The number of privacy reviews completed during each reporting period are noted below. Generally, the total number of privacy reviews has been steady across each reporting period. There are changes in certain types of reviews, however. Notably, many categories of privacy reviews are initiated by Components, and categories can change based on several factors, including: changes in Administration priorities; significant events, like a public health emergency or catastrophic event; and Component Privacy Offices' resources.

Table I Privacy Reviews Completed:			
Type of Review	***Number of Reviews***		
	1st Half of FY 2022 ***October 2021 – March 2022***	**2nd Half of FY 2022** ***April 2022 – September 2022***	**1st Half of FY 2023** ***October 2022 – March 2023***
Privacy Threshold Analyses	1039	991	947
Privacy Impact Assessments	15	11	10
System of Records Notices and associated Privacy Act Exemptions	9	5	1
Privacy Act (e)(3) Statements[13]	90	122	173
Computer Matching Agreements[14]	7	2	1
Privacy Compliance Reviews	0	0	0
Information Technology Acquisition Reviews (ITAR)	150	223	211
Other Privacy Reviews	0	0	0
Total Reviews	1310	1354	1343

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

[14] Computer Matching Agreements are typically renewed or re-established.

Privacy Impact Assessments

The Privacy Impact Assessment process is one of the Department's key mechanisms to ensure that DHS programs and technologies embed privacy 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 conducts a triennial review of existing Privacy Impact Assessments to assess and confirm systems' operations are consistent with the original assessment and corresponding privacy safeguards. Following the triennial review, the Department updates previously published Privacy Impact Assessments to inform the public it has completed a review of affected systems.

As of March 31, 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.[15]

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

October 1, 2021 – March 31, 2022

DHS/ICE/PIA-060 ICE Body Worn Camera (BWC) Pilot *(November 2, 2021)*
ICE conducted a Body Worn Camera (BWC) Pilot at select field office locations: three within the Office of Enforcement and Removal Operations (ERO) and three within the Office of Homeland Security Investigations (HSI) (collectively, ICE). The ICE Office of Firearms and Tactical Programs coordinated the effort among the respective ICE program offices and is responsible for the training, testing, evaluation, and oversight of the Body Worn Camera Pilot. The purpose of the Body Worn Camera Pilot is to examine the operational feasibility of an ICE enterprise-wide Body Worn Camera requirement by identifying the costs and benefits, including workload impacts, time commitment, and logistical challenges associated with implementation. The initial goals of the Pilot are to determine the effectiveness of using Body Worn Camera technology to provide an accurate representation of ICE law enforcement encounters while allowing ICE field personnel to safely perform their duties. This pilot will be executed in an operational environment; therefore, any data collected in support of enforcement activity during the Pilot will be used to support the ICE mission. ICE published this Privacy Impact Assessment to evaluate the privacy risks associated with the potential use of Body Worn Camera technology on a wider scale and to address any issues related to the product selection, collection, retention, and storage of the information collected from Body Worn Camera usage.

DHS/TSA/PIA-050 Amtrak Rail Passenger Threat Assessment *(December 1, 2021)*
TSA is responsible for security in all modes of transportation, including surface modes such as rail. Amtrak is a national passenger rail operator managing more than 300 trains a day traveling to more than 500 destinations in the United States and Canada. To evaluate the operating environment from a risk

[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 DHS Privacy Office.

perspective, Amtrak has requested that TSA assess the use of Amtrak trains by known or suspected terrorists. To conduct the assessment, Amtrak will provide TSA with the personally identifiable information of rail passengers collected over several months for TSA to match against the Threat Screening Center's (TSC) Terrorist Screening Database (TSDB), commonly known as the "watchlist." TSA conducted this Privacy Impact Assessment pursuant to the E-Government Act of 2002 because this assessment entails a new receipt of personally identifiable information on members of the public for watchlist matching.

DHS/ALL/PIA-092 Immigrant Military Members and Veterans Initiative (IMMVI) *(January 26, 2022)*
On February 2, 2021, President Biden signed Executive Order 14012, "Restoring Faith in Our Legal Immigration Systems and Strengthening Integration and Inclusion Efforts for New Americans." In support of Executive Order 14012, on July 2, 2021, the Secretaries of DHS and Veterans Affairs (VA) announced a new joint initiative, the Immigrant Military Members and Veterans Initiative. This initiative was formed to support the Nation's noncitizen service members, and their immediate family members, and directed DHS and the VA to identify and prioritize the return of current and former U.S. military members, and their immediate family members, who were removed from the United States, to ensure they receive the benefits to which they may be entitled. This Privacy Impact Assessment analyzed the privacy risks associated with the personally identifiable information collected as part of this effort and documented the mitigation strategies implemented to ensure appropriate protection of those individuals' privacy.

DHS/S&T/PIA-042 DHS Federally Funded Research and Development Centers *(February 22, 2022)*
DHS sponsors federally funded research and development centers (FFRDC). The DHS Science and Technology Directorate (S&T) FFRDC Program Management Office oversees and manages access to these specialized services in systems engineering, integration, studies, and analysis. The FFRDC services can be accessed by DHS Components; external federal, state, and local government; non-governmental organizations and institutions; universities and affiliated research centers; and other public sector and private sector groups, through the Program Management Office. S&T conducted this Privacy Impact Assessment to address the Department's FFRDC program, two specific FFRDCs (i.e., Homeland Security Operational Analysis Center and Homeland Security Systems Engineering and Development Institute), and the privacy risks associated with the collection, use, maintenance, and dissemination of personally identifiable information, privacy sensitive projects and activities, and use of DHS-accredited information systems.

April 1, 2022 – September 30, 2022
DHS/CBP/PIA-072 Unified Immigration Portal *(April 1, 2022)*
The U.S. immigration system is complex, involving multiple federal government stakeholders, processes, and information technology systems. This complexity creates challenges between agencies involved in the immigration process that need to share and receive comprehensive, consistent, and timely information required to make impactful and mission-critical decisions. The CBP Unified Immigration Portal provides agencies involved in the immigration process a means to view and access certain information from each of the respective agencies from a single portal in near real-time (as the information is entered into the source systems). CBP published this Privacy Impact Assessment to provide notice of implementation of the Unified Immigration Portal and assess the privacy risks and mitigation measures for the Portal.

DHS/ALL/PIA-093 Hummingbird *(April 11, 2022)*
On August 29, 2021, President Biden directed DHS to lead the implementation of ongoing efforts across the federal government to support vulnerable Afghans, including those who worked alongside the United States in Afghanistan for the past two decades, as they safely resettle in the United States. These coordinated efforts are collectively known as Operation Allies Welcome. The leadership of the program is transitioning from the Department of State (State) to DHS. To support its Operation Allies Welcome responsibilities, DHS will use the Hummingbird application as a tool for tracking, screening, processing, and resettling individuals from Afghanistan who are neither U.S. citizens nor lawful permanent residents. This Privacy Impact Assessment was conducted to analyze the privacy risks associated with the collection of personally identifiable information necessary for the success of Operation Allies Welcome and to document the mitigation strategies implemented to ensure appropriate protection of participants' privacy.

DHS/ALL/PIA-094 Migrant Protection Protocols (MPP) Case Request System (*May 20, 2022*)
Migrant Protection Protocols is a United States government program initiated in January 2019 pursuant to Section 235(b)(2)(C) of the Immigration and Nationality Act. Under Migrant Protection Protocols, the United States returns certain citizens and non-Mexican nationals to Mexico while their U.S. removal proceedings are pending. The Migrant Protection Protocols Case Request System provides an avenue for individuals to initiate a review of their enrollment in the program if they believe they should not be in the program. This Privacy Impact Assessment was conducted to analyze the privacy risks associated with the collection of personally identifiable information as part of this effort and document the mitigation strategies implemented to ensure appropriate protection of those individuals' privacy.

October 1, 2022 – March 31, 2023
DHS/CBP/PIA-073 Advance Travel Authorization *(October 17, 2022)*
DHS developed a new, voluntary Advance Travel Authorization process to collect information from eligible noncitizens requesting advance authorization to travel to the United States to seek a discretionary grant of parole. CBP published this new Privacy Impact Assessment to provide notice and assess the privacy risks associated with Advance Travel Authorization. Advance Travel Authorization launched on October 12, 2022, to implement a parole process for certain undocumented noncitizens from select countries and their qualifying immediate family members under which those individuals may request advance authorization to travel to the United States to seek a discretionary grant of parole. This Privacy Impact Assessment discusses the general workflow of Advance Travel Authorization and the information collected, stored, and used at each step. CBP's Advance Travel Authorization collection is conducted through the CBP One™ mobile application, and CBP published a CBP One™ Privacy Impact Assessment appendix update concurrently with this Advance Travel Authorization Privacy Impact Assessment.

DHS/ALL/PIA-095 DHS International Biometric Information Sharing (IBIS) Program Information Sharing (IBIS) Program *(November 2, 2022)*
DHS Office of Strategy, Policy, and Plans, in cooperation with DHS Components, created the International Biometric Information Sharing Program to enhance cooperation between DHS Components and foreign partners in assessing the eligibility or public security risk of individuals seeking an immigration benefit or encountered in the context of a border encounter or law enforcement investigation related to immigration or border security issues. DHS created the International Biometric Information Sharing Program to improve the Department's and its foreign partners' ability to more definitively establish the identity and assess the eligibility of an individual presenting for an immigration benefit or when encountered by DHS law enforcement in border and immigration-related contexts. The

ability of biometric information sharing to support law enforcement investigations and immigration benefit decisions is validated in DHS's current international partnerships. This information has assisted foreign partners in detecting identity fraud, foreign criminals who have not disclosed their prior criminal activity, and known or suspected terrorists. This Privacy Impact Assessment considers the privacy risks and applicable mitigation strategies associated with implementing this Departmental program.

DHS/CBP/PIA-075 Intelligent Computer-Assisted Detection (ICAD) System *(November 3, 2022)*
CBP operates the Intelligent Computer-Assisted Detection system to provide situational awareness along the United States border. The Intelligent Computer-Assisted Detection system assists the United States Border Patrol in detecting, identifying, and apprehending individuals who may have illegally entered the United States or otherwise violated applicable U.S. laws between ports of entry. CBP provided notice to members of the public about the Intelligent Computer-Assisted Detection system in the Border Surveillance Systems Privacy Impact Assessment and published this new document to provide transparency of the system's application and functionality.

DHS/USCIS/PIA-087 Person Centric Identity Services (PCIS) Initiative *(December 7, 2022)*
USCIS is implementing Person Centric Identity Services, an agency-wide effort to use enhanced business processes and emerging technologies to improve the reliability, accuracy, and completeness of biographic and biometric information across USCIS and other DHS immigration-related systems. The Person Centric Identity Services system compiles and aggregates this declared and obtained data using algorithms and other sophisticated tools to establish an identity profile. The identity profile presents a single data set of consistent information about an individual's identity history as essential support for adjudicative efficiency.

There are limitations inherent in the current USCIS process of linking declared identity data solely to an individual's assigned identifier, which can lead to incomplete or unreliable records. To improve completeness and reliability, USCIS is leveraging existing Information Technology (IT) systems and using Person Centric Identity Services to enhance identity management across USCIS and other DHS components that rely on immigration records to accomplish their missions. The initial version of Person Centric Identity Services was released into production in November 2021 and consisted of the Identity Population Pipeline, the Identity Index, Core Search, and User Interface basic functions. USCIS published this Privacy Impact Assessment to describe the overall approach and vision for Person Centric Identity Services and the personally identifiable information it plans to collect, use, maintain, and share. USCIS is developing Person Centric Identity Services in incremental phases and plans to update the Privacy Impact Assessment, as appropriate, to assess the privacy risks associated with future development efforts.

DHS/CBP/PIA-076 Collection of Advance Information from Certain Undocumented Individuals on the Land Border *(January 19, 2023)*
Historically, CBP received no advance biographic or biometric information before the arrival of undocumented individuals at ports of entry. This lack of information increases the amount of time it takes CBP officers to process undocumented individuals upon their arrival. To streamline and increase processing capacity at land ports of entry, CBP is expanding the use of the CBP One™ mobile and desktop application to allow the advanced submission of biographic and biometric information from undocumented individuals seeking admission into the United States. Undocumented individuals, organizations, and entities (e.g., International Organizations and Non-Governmental Organizations) acting on their behalf may voluntarily submit biographic and biometric information via CBP One™. CBP previously provided notice of this advance information collection through a Privacy Impact

Assessment Update to DHS/CBP/PIA-067(a) Unified Secondary and Privacy Impact Assessment Appendices to the DHS/CBP/PIA-056 Traveler Verification Service and DHS/CBP/PIA-068 CBP One™ Mobile Application. CBP conducted this new standalone Privacy Impact Assessment to provide full transparency on this initiative and fully assess the risks associated with this collection.

DHS/CBP/PIA-077 CBP Broker Management Program *(March 31, 2023)*
The CBP Office of Trade oversees the CBP Broker Management Program. The program collects personally identifiable information from individuals when: they register to take the Customs Broker License Exam (either in-person or remotely); during the administration of the Customs Broker License Exam; when applying for a Customs broker license; throughout the background investigation processes; through the triennial reporting process; through any continuing education requirements; and through the entire time the license is held. CBP published this overarching Privacy Impact Assessment to: (1) document the procedures to become a federally licensed Customs broker, as well as the associated duties and responsibilities; (2) provide notice of a new collection and maintenance of information (audio and video recordings) from individuals taking the Customs Broker License Exam remotely; and (3) to fully discuss the use of Artificial Intelligence (AI) during remotely administered Customs Broker License Exams.

Updated Privacy Impact Assessments

October 1, 2021 – March 31, 2022
DHS/CBP/PIA-013(a) Customs Trade Partnership Against Terrorism *(January 3, 2022)*
The Customs Trade Partnership Against Terrorism is a CBP voluntary trade partnership program in which CBP and members of the trade community work together to secure and facilitate the movement of legitimate international trade. The program focuses on improving security throughout the supply chain, beginning at the point of origin (including manufacturer, supplier, or vendor), through the distribution, to the destination. Customs Trade Partnership Against Terrorism member companies, called partners, agree to implement security procedures throughout their supply chains to protect those supply chains from terrorist infiltration and other illegal activities that threaten the security of the United States. CBP published this Privacy Impact Assessment Update to provide notice of: (1) the Customs Trade Partnership Against Terrorism Trade Compliance Program; (2) the collection of additional data elements for the Customs Trade Partnership Against Terrorism Security Program; and (3) an update to the proposed National Archives and Records Administration records retention schedule.

DHS/ICE/PIA-046(a) Laboratory Information Management System *(February 1, 2022)*
ICE Office of Homeland Security Investigations (HSI) owns and operates the Laboratory Information Management System as part of its Forensic Laboratory. The HSI Forensic Laboratory implemented the Laboratory Information Management System to facilitate and store data related to the scientific authentication, examination, research, and analysis of documents and the enhancement of audio-visual materials. HSI Forensic Laboratory also examines latent finger and palm prints found in the field. ICE published this Privacy Impact Assessment Update to provide transparency regarding a new subsystem within the Laboratory Information Management System called LatentCD, which allows the HSI Forensic Laboratory Latent Print Unit to ingest and manage the workflow of unidentified latent prints.

April 1, 2022 – September 30, 2022
DHS/USCG/PIA-028(a) Defense Sexual Assault Incident Database *(July 29, 2022)*
The Department of Defense (DoD) owns and operates the Defense Sexual Assault Incident Database system, a centralized, case-level database for military sexual assault reports. The system is a case

management and business management tool that contains information provided by all military services and provides information that is used to build metrics and track cases from start to conclusion. The system collects and maintains personally identifiable information about U.S. Coast Guard (USCG) personnel and other individuals involved. USCG updated this Privacy Impact Assessment because the Defense Sexual Assault Incident Database now collects and maintains personally identifiable information about USCG civilian personnel.

DHS/ALL/PIA-048(c) Foreign Access Management System *(August 15, 2022)*
The DHS Under Secretary for Management (USM), Office of the Chief Security Officer (OCSO), and Center for International Safety and Security (CISS) manage the Foreign Access Management program that vets foreign nationals, foreign entities, and certain United States Persons that seek access to DHS personnel, information, facilities, programs, or systems. This PIA Update reflects the end of the Foreign Access Management Enterprise Pilot program and the end of the agreement between OCSO/CISS and the Office of the Director of National Intelligence (ODNI) National Counterintelligence and Security Center.[16] This PIA update also covers the addition of systems that include the CISS vetting process; an increase in the foreign contact reporting population based on Security Executive Agent Directive (SEAD) 3, which expanded reporting requirements to DHS employees and contractors (covered individuals) holding sensitive positions; and a discussion on CISS's use of Tableau as a dashboard for DHS security personnel.

October 1, 2022 – March 31, 2023
DHS/TSA/PIA-046(d) Travel Document Checker Automation Using Facial Identification Automation *(November 17, 2022)*
TSA, in partnership with CBP, is expanding the use of facial identification technology to enhance the identity verification process at TSA checkpoints. TSA's proof of concept employs a Credential Authentication Technology (CAT) device equipped with a camera (referred to as CAT-2), along with biometric matching services provided by CBP's Traveler Verification Service (TVS), to verify the identities of certain travelers who opt-in during check-in at the Detroit Metropolitan Wayne County Airport in partnership with Delta Airlines. This Privacy Impact Assessment update reflects expanding this concept to additional locations and airlines and includes a proof of concept that does not require participating passengers to scan their identity documents.

DHS/ALL/PIA-095(a) DHS International Biometric Information Sharing Program (IBIS) - Biometric Data Sharing Partnerships (BDSP) *(November 18, 2022)*
As noted above, DHS Office of Strategy, Policy, and Plans, in cooperation with DHS Components, created the International Biometric Information Sharing Program to support DHS Components and foreign partners in assessing the eligibility or public security risk of individuals seeking an immigration benefit in the context of a border encounter or law enforcement investigation related to immigration or border security issues. This Privacy Impact Assessment Update considers the privacy risks and mitigation strategies associated with implementing this Departmental program in cases where partners permit DHS to retain all biometric enrollments regardless of a match to an existing DHS record, as this

[16] The discontinuation of the Foreign Access Management Enterprise Pilot program resulted from project scope, feasibility, and funding issues between ODNI and DHS. The agreement between ODNI and DHS OCSO has been terminated. Foreign national data collection did not occur because the pilot never became operational.

additional collection differs from the scope covered by the original International Biometric Information Sharing Program Privacy Impact Assessment.

DHS/TSA/PIA-029(b) TSA Operations Center Information Management System Management System *(December 5, 2022)*
TSA Transportation Security Operations Center serves as TSA's coordination center for transportation security incidents and operations. The Transportation Security Operations Center uses the Web-Based Emergency Operations Center incident management system to perform incident management, coordination, and situational awareness functions for all modes of transportation. The system maintains information including personally identifiable information. The system also collects and compiles reports from federal, state, local, tribal, foreign, and international sources and private sector security officials on incidents related to transportation or national security threats. TSA updated this Privacy Impact Assessment to reflect the addition of several new collections of personally identifiable information.

DHS/USCIS/PIA-062(a) Administrative Appeals Office Case Management System *(January 30, 2023)*
USCIS Administrative Appeals Office uses the Administrative Appeals Office Case Management System to capture and track information related to appeals, motions, and certifications that the Administrative Appeals Office adjudicates under its jurisdiction and to improve its ability to track appeals and case processing. USCIS conducted this Privacy Impact Assessment update to account for the capture of additional information in the Case Management System and identify the privacy risks and mitigations associated with the collection and use of this additional information.

System of Records Notices

The Department publishes System of Records Notices consistent with requirements outlined in the *Privacy Act of 1974,* as amended.[17] The Department conducts assessments to ensure System of Records Notices remain accurate, up-to-date, and appropriately scoped. 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 March 31, 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 published three new System of Records Notices and three associated Privacy Act rulemakings during the reporting period.

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

New System of Records Notices

October 1, 2021 – March 31, 2022
DHS/OIG-002 Investigative Records System

[17] 5 U.S.C. § 552a(e)(4), (j), (k). *See also* OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," 81 Fed. Reg. 94424 (Dec. 23, 2016), *available at*: https://www.gpo.gov/fdsys/pkg/FR-2016-12-23/pdf/2016-30901.pdf.

This system of records allows DHS Office of Inspector General (OIG) to collect and maintain records related to alleged violations of criminal, civil, and administrative laws and regulations pertaining to DHS programs, operations, and employees, contractors, and other individuals and entities associated with DHS; monitor complaint and investigation assignments, status, disposition, and results; manage investigations and information provided during investigations; audit actions taken by DHS management regarding employee misconduct and other allegations; audit legal actions taken following referrals to the U.S. Department of Justice for criminal prosecution or litigation; provide information relating to any adverse action or other proceeding that may occur as a result of the findings of an investigation; and provide a system for calculating and reporting statistical information. DHS OIG updated this System of Records Notice to provide notice of changes to the Authorities, Categories of Records, Record Source Categories, and Routine Uses. *(86 FR 58292, October 21, 2021).*

DHS/FEMA-008 Disaster Recovery Assistance Files
This System of Records Notice describes FEMA's collection and maintenance of records on applicants for its Disaster Assistance programs that provide financial and other tangible assistance to survivors of presidentially declared disasters or emergencies. FEMA modified this System of Records Notice to: (1) update the system location; (2) clarify the purpose of the System of Records Notice; (3) update the categories of records; (4) update the routine uses; (5) change the retention and disposal schedule of records; and (6) update record source categories. Additionally, this notice included non-substantive changes to simplify the formatting and text of the previously published notice. *(87 FR 7852, February 10, 2022).*

DHS/S&T-001 Research, Development, Test, and Evaluation Records
This system of records supports the collection of records for the S&T-funded Research Development Test and Evaluation (RDT&E) activities in support of DHS Components and other partners in the Homeland Security Enterprise. Records are collected through RDT&E activities such as testing and evaluating a screening technology, obtaining feedback on a technology from volunteer participants, or evaluating analytic tools using publicly available information. *(86 FR 58084, October 20, 2021).*

April 1, 2022 – September 30, 2022
DHS/ALL-033 Reasonable Accommodations System of Records
This system of records allows the Department to collect and maintain records on employees and applicants for employment who requested or received reasonable accommodations by the Department as required by the Rehabilitation Act of 1973, as amended; the Americans with Disabilities Act Amendments of 2008; Title VII of the Civil Rights Act, as amended; and/or pursuant to public health authorities and associated guidance. DHS updated this System of Records Notice to provide more transparency to its purpose; add additional authorities for the collection of information; update the categories of records; modify and add routine uses; and update retention policies. This notice also clarified DHS's collection, use, maintenance, and dissemination of records needed to process, manage, maintain, and resolve reasonable accommodation requests based on a medical condition/disability or a sincerely held religious belief, practice, or observance. *(87 FR 19111, April 1, 2022).*

DHS/FEMA-004 Non-Disaster Grant Management Information Files System of Records
This system of records allows FEMA to collect and maintain records collected from state, local, tribal, territorial, and other entities applying for non-disaster related FEMA grant programs. FEMA collects grant management information to determine eligibility for DHS grant awards for non-disaster grants and the issuance of awarded funds. FEMA updated this System of Records Notice to revise and add routine uses and update the retention schedule. *(87 FR 41141, July 11, 2022).*

October 1, 2022 – March 31, 2023
DHS/CBP-027 Customs Broker Management (CBM)
The purpose of this system is to maintain information about individuals to determine: (1) an individual's suitability for acquiring a Customs Broker license, whether that individual is representing themself or affiliated with an association, corporation, or partnership and (2) whether a licensed Customs Broker continues to meet the eligibility requirements to maintain that Customs Broker license. *(88 FR 19213, March 31, 2023).*

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. The Privacy Office has issued nearly 130 recommendations through the Privacy Compliance Review process. More than 110 of the recommendations have been closed based on responses from Component Privacy Officers and Privacy Points of Contact.

Working Group Participation

The following chart summarizes Privacy Office participation in DHS working groups throughout the reporting period.

Body	Description	Privacy Office Participation
Data Services Branch (DSB)	The DSB is the center of excellence for customized data services to help generate insights and value of data. The mission is to provide infrastructure, tools, and knowledge to deliver data analytics capabilities and services for DHS Headquarters and Components.	The Privacy Office facilitates the preservation of privacy protections with DSB through: - Privacy Threshold Analysis submissions for each dataset targeted for onboarding, as well as updates to the DSB Privacy Impact Assessment and System of Records Notice for each dataset onboarded for any new use or user of a dataset. -Approval of all datasets ingested. Requestors must provide an articulated use consistent with the use or uses approved by the IT source system as a member of the DSB Working Group. -Approval of all bulk data transfers to ensure information sharing is governed by appropriate safeguards in accordance with the Fair Information

		Practice Principles through coordination with the Data Access Review Council (DARC).
Data Stewardship Working Groups (DSWGs)	The DSWG is an outgrowth of the Immigration Data Integration Initiative Data Governance Working Group. The DSWGs are responsible for each data set mission.	The Privacy Office is a member of several DSWGs where the dataset(s) contains or leverages personally identifiable information. Specifically, the Privacy Office Policy & Oversight team developed and edited the Immigration Data Integration Initiative Data Stewards' training material to address education, identification, and mitigation of privacy risks. Privacy-focused areas in the training included: data disclosure limitations and constraints; purpose of and requirements for privacy compliance documentation; and oversight office roles and responsibilities.
Body	**Description**	**Privacy Office Participation**
Risk and Resilience Policy Council (R2PC)	The R2PC identifies emerging risks consisting of threats and opportunities most likely to impact homeland security over the next two to five-year planning cycle. Along with risk identification, the Council seeks to mitigate inherent uncertainty, support planning, guide investment, and foster collaboration.	As risk mitigation activities develop, the Privacy Office will continue to focus on the safeguards around the use of sensitive personally identifiable information, the impact on the individual, and compliance with privacy laws and policies.
Privacy, Civil Rights, and Civil Liberties (PCRCL) Working Group of the National Vetting Center (NVC)	The PCRCL Working Group is comprised of senior privacy and civil liberties officials from several departments and agencies supporting the implementation of NSPM-9, *Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise.*	The Chief Privacy Officer serves as co-chair of the PCRCL Working Group and represents the PCRCL Working Group as an *ex officio*, non-voting member of the National Vetting Center (NVC) Governance Board. The Working Group meets regularly to evaluate screening and vetting program proposals, the attendant implementation plans, Concepts of Operations, and technology structures to ensure NVC activities are conducted in a privacy-protective manner.
Targeted Violence and Terrorism Prevention (TVTP) Working Group	The TVTP Working Group provides a forum for DHS Components and Offices to collaborate on TVTP policies and strategies and to develop cross-Component TVTP implementation plans, approaches, and initiatives to support the core objectives of	The Privacy Office's participation in this Working Group ensures that the Department's actions to prevent targeted violence and terrorism respect an individual's privacy, civil rights, and civil liberties, and are developed, evaluated, coordinated, integrated, aligned, and implemented in accordance with applicable Department governance.

	the Department's *2019 Strategic Framework for Countering Terrorism and Targeted Violence* and national strategies.	

COMPONENT PRIVACY AWARENESS INITIATIVES

Cybersecurity and Internet Security Agency (CISA)

October 1, 2021 – March 31, 2022

- On October 6, 2021, the CISA Chief Privacy Officer discussed privacy considerations in cybersecurity and CISA's implementation of recent cybersecurity Executive Orders during the Privacy 15Connect's chapter meeting.
- On October 13, 2021, the CISA Chief Privacy Officer participated in the Government Huddle podcast, speaking on topics related to CISA's privacy role and implementation of recent cybersecurity Executive Orders.
- On October 21, 2021, the CISA Office of the Chief Privacy Officer participated in the DHS IT Acquisition Review Conference. Privacy analysts conducted privacy training for contracting officials across DHS regarding the privacy review in the Information Technology Acquisition Review (ITAR) process.
- On October 27, 2021, the CISA Office of Chief Privacy Officer participated in the CISA ITAR Refresher Training. Privacy analysts conducted privacy training for CISA employees regarding the privacy review in the ITAR process.
- On November 5, 2021, the CISA Office of the Chief Privacy Officer trained employees from the CISA's Threat Hunting team on Privacy Act requirements. This training included how to determine if a System of Record Notice is needed and the requirements for access and redress that must be afforded to individuals.
- On November 24, 2021, the CISA Chief Privacy Officer delivered a keynote address on privacy considerations for digital identity management for the Public Sector Network's Digital Identity event.
- In this reporting period, 359 CISA employees completed *the Cybersecurity Information Handling Guidelines Training*, created by CISA's Office of the Chief Privacy Officer and CISA's Office of Chief Counsel.
- Finally, the CISA Office of the Chief Privacy Officer issued the quarterly privacy newsletter, the CISA Privacy Update. The newsletter is distributed CISA-wide and posted on the CISA Office of Chief Privacy Officer's internal intranet page.

April 1, 2022 – September 30, 2022

- In this reporting period, 380 CISA employees completed the *Cybersecurity Information Handling Guidelines Training*, created by CISA's Office of the Chief Privacy Officer and CISA's Office of Chief Counsel.
- The CISA Office of the Chief Privacy Officer released quarterly privacy newsletters. The newsletter is distributed CISA-wide and posted on the CISA Office of Chief Privacy Officer's internal intranet page.

- On August 23, 2022, the CISA Office of Chief Privacy Officer organized the CISA Privacy Incident Awareness & Response Training. Privacy analysts conducted an agency-wide privacy training for all CISA employees to review how to identify a privacy incident, the incident reporting process, and best practices in safeguarding personally identifiable information while teleworking or at the office.
- In this reporting period, 75 CISA employees from regional offices completed the *Administrative Subpoena Module 1* training. This training was created by CISA's Joint Cyber Defense Collaborative, Office of Chief Counsel, and Office of the Chief Privacy Officer. It included information on the handling and protection of personally identifiable information in the administrative subpoena process.

October 1, 2022 – March 31, 2023

- On November 15, 2022, 41 CISA employees and contractors participated in a CISA Privacy Incident Refresher Training for Executive Secretariat Taskers conducted by the CISA Office of Privacy, Access, Civil Liberties, and Transparency.
- On February 16, 2023, 8 CISA employees and contractors within the Infrastructure Security Division participated in a CISA Privacy Incident Refresher Training for Executive Secretariat Taskers conducted by the CISA Office of Privacy, Access, Civil Liberties, and Transparency.

Science and Technology Directorate (S&T)

October 1, 2021 – March 31, 2022

- S&T conducted four training sessions for employees from S&T, Customs and Border Protection, Cybersecurity and Infrastructure Security Agency, Office of Inspector General, Federal Emergency Management Administration, Transportation Security Administration, and the United States Secret Service to assist with their mandatory transition to the Homeland Security Systems Engineering and Development Institute IT Enclave for activities related to federally funded research and development centers (FFRDC).
- S&T provided two training sessions to the Royal Canadian Mounted Police who use the Integrated Maritime Domain Enterprise as part of their work with the Great Lakes Marines Security Operating Center.
- S&T provided annual privacy training to RAND and DHS employees in connection with the FFRDC Homeland Security Operation and Analysis Center.
- S&T provided privacy awareness training to S&T's Tech Scouting and Transition division and identified areas with which the division can assist integrating privacy requirements into project lifecycles, ensuring a smoother transition from research to operational use.

April 1, 2022 – September 30, 2022

- S&T provided two Privacy Awareness Training sessions for the Office of University Programs and the Program Manager User Group on shared privacy responsibilities, privacy sensitivity, and the safeguarding of personally identifiable information.
- S&T conducted two training sessions for DHS employees from CISA and FEMA on the mandatory transition to the Homeland Security Operation and Analysis Center IT Enclave for FFRDC-related activities.
- S&T collaborated on a Brown Bag Training for employees regarding the Privacy Office's review process during the Foreign Disclosure Office Review.
- S&T provided three Privacy Awareness Training sessions to the S&T Technology Centers Division on shared privacy responsibilities, privacy sensitivity, and the safeguarding of personally identifiable information.

- S&T conducted Privacy Awareness training for its Chief of Staff.
- S&T provided training on all functions of the S&T Privacy Program to support the onboarding of the new S&T Under Secretary and Chief Scientist.

October 1, 2022 – March 31, 2023

- S&T collaborated with the Office of Procurement Operations and the Science and Technology Acquisition Division to provide Directorate-wide training on the Privacy Office role in the purchase requisition review process.
- S&T conducted four training sessions on the mandatory transition to the Homeland Security Operation and Analysis Center IT Enclave for FFRDC-related activities for DHS employees from all Components.

Transportation Security Administration (TSA)

October 1, 2021 – March 31, 2022

- TSA conducted training for 93 Information Systems Security Officers (ISSOs) on how to prepare a Privacy Threshold Analysis.
- TSA conducted training for 94 reviewers on privacy considerations in processing reasonable accommodations requests.
- TSA conducted outreach to privacy advocacy groups on a variety of TSA topics.

April 1, 2022 – September 30, 2022

- TSA conducted training for 70 Intelligence staff members on First Amendment and civil liberties issues when preparing Intelligence Products.
- TSA conducted training for 49 reviewers on privacy considerations in processing reasonable accommodations requests.
- TSA conducted training for Counter-Intelligence staff members on data sharing issues.
- TSA participated in the TSA Biometric Identity Management Summit with more than 300 industry and privacy advocate groups.
- TSA conducted outreach to privacy advocacy groups on a variety of TSA topics, including TSA use of biometrics, Amtrak passenger assessment, non-discrimination policies, and use of watchlists.

October 1, 2022 – March 31, 2023

- TSA conducted training for 70 Intelligence staff members on First Amendment and civil liberties issues when preparing Intelligence Products.
- TSA conducted training for 149 Information Systems Security Officers (ISSOs) on how to prepare a Privacy Threshold Analysis.
- TSA conducted outreach to privacy advocacy groups on a variety of TSA topics, including TSA use of biometrics, Amtrak passenger assessment, and use of watch lists/rules-based screening.

U.S. Citizenship and Immigration Services (USCIS)

October 1, 2021 – March 31, 2022

- USCIS provided computer-based and instructor-led Privacy Awareness Training to 3,261 personnel. These training sessions included:
    - Multiple instructor-led Privacy Awareness Training sessions as part of its support to Field Operations, Service Center Operations, and HQ Operations.

    - Instructor-led privacy awareness training for the New Employee Orientation Program. This training is provided to new employees onboarding at USCIS Headquarters, Field Offices, and Services Centers.
    - Instructor-led privacy awareness training for the Fundamentals of Mission Support Training Program. This training is provided to Mission Support Specialists and Operations Support Specialists.
- In this reporting period, 67 USCIS employees completed Privacy Requirements for Operational Use of Social Media.
- USCIS conducted multiple training sessions for stakeholders (e.g., system development teams, project teams, and information system security officers, etc.) on how to complete privacy compliance documentation, including multiple specialized trainings on the development of Privacy Threshold Analyses.
- USCIS developed and conducted specialized training regarding the integration of privacy and data security principles in information sharing activities. This training was provided to the Identity and Information Management Division, Interagency and International Information Sharing Branch team, and the Office of the Chief Data Officer to discuss the privacy requirements for each agreement, an overview of foundational privacy laws/guidance, applicable privacy compliance documents, and a list of issues Privacy assesses when reviewing information sharing agreements.
- USCIS conducted training on the development of a Privacy Threshold Analysis for the USCIS Information Collection and Paperwork Reduction Act Working Group. This training provided a comprehensive review of the Privacy Threshold Analysis template and provided nuanced instructional information for one of the Office of Privacy's primary customers.
- USCIS conducted training on how the Office of Privacy reviews agency's contracts to identify privacy risks, the completion of the Department of Homeland Security Acquisition Manual Appendix G Form, and how to determine if the Homeland Security Acquisition Regulation clauses are required. The training was provided to Contracting Officers and Contracting Officer's Representatives on March 20, 2022.
- USCIS developed a privacy newsletter on the importance of protecting privacy for Data Privacy Day that was distributed to the USCIS Directorates and Program Offices on January 28, 2022.

April 1, 2022 – September 30, 2022

- USCIS provided computer-based and instructor-led Privacy Awareness Training to 21,673 personnel. These training sessions included:
    - Multiple sessions of instructor-led Privacy Awareness Training as part of its support to Field Operations, Service Center Operations and Headquarters Operations.
    - Instructor-led privacy awareness training for the New Employee Orientation Program.
    - Instructor-led privacy awareness training for the Fundamentals of Mission Support Training Program.
- In this reporting period, 188 USCIS employees completed Privacy Requirements for Operational Use of Social Media.
- USCIS conducted multiple training sessions for stakeholders (e.g., system development teams, project teams, and information system security officers, etc.) on how to complete privacy compliance documentation, including multiple specialized trainings on the development of Privacy Threshold Analyses.
- USCIS conducted specialized training for the Digital Innovation Development – Information Technology development team regarding privacy compliance requirements for their system, including a detailed analysis of how to monitor/maintain privacy compliance for approximately 75 applications within the authorization boundary.

- USCIS conducted specialized integration of privacy and data security principles training for the Office of Chief Counsel. This training focused on privacy requirements for agreements, applicable privacy compliance documents, and a comprehensive list of the privacy issues assessed in information sharing agreements.
- USCIS developed and conducted a training course to provide in-depth information on the legal foundations of privacy, including applicable laws, Office of Management and Budget memoranda, and DHS policies, and how they are incorporated into the daily responsibilities of USCIS privacy professionals. The purpose of the training was to ensure all USCIS privacy team members and other interested USCIS Program Office and Directorate employees are fully trained on privacy.
- USCIS developed and conducted a training course to provide in-depth training on the privacy requirements for information sharing agreements, Privacy Threshold Analyses, Information Sharing Agreement Privacy Threshold Analyses, Decommissioning Privacy Threshold Analyses, Privacy Impact Assessments, Privacy Notices, and System of Records Notices. This training course and each module were recorded for future use.
- USCIS conducted training on developing a Privacy Threshold Analysis for the USCIS Information Collection and Paperwork Reduction Act Working Group. This training provided a comprehensive review of the Privacy Threshold Analysis template and provided nuanced instructional information for one of the Office of Privacy's primary customers.
- USCIS developed "Privacy Tips" and posted them via digital signage and on the USCIS Connect Site.

October 1, 2022 – March 31, 2023

- USCIS provided computer-based and instructor-led Privacy Awareness Training to 3,218 personnel. These training sessions included:
    - Multiple sessions of instructor-led Privacy Awareness Training as part of its support to Field Operations, Service Center Operations, and Headquarters Operations.
    - Instructor-led privacy awareness training for the New Employee Orientation Program.
    - Instructor-led privacy awareness training for the Fundamentals of Mission Support Training Program.
- In this reporting period, 93 USCIS employees completed Privacy Requirements for Operational Use of Social Media.
- USCIS conducted multiple training sessions for stakeholders (e.g., system development teams, project teams, and information system security officers, etc.) on how to complete privacy compliance documentation, including multiple specialized trainings on the development of Privacy Threshold Analyses.
- USCIS conducted training on developing a Privacy Threshold Analysis for the USCIS Information Collection and Paperwork Reduction Act Working Group. This training provided a comprehensive review of the Privacy Threshold Analysis template and provided nuanced instructional information for one of the Office of Privacy's primary customers.
- USCIS conducted training on how the Office of Privacy reviews the agency's contracts to identify privacy risks, the completion of the Homeland Security Acquisition Manual Appendix G Form, and how to determine if the Homeland Security Acquisition Regulation clauses are required. The training was conducted for Contracting Officers and Contracting Officer's Representatives.
- USCIS provided privacy briefings to new field office directors on the USCIS Office of Privacy's mission and goals, including how the regional privacy officers can assist with ensuring compliance with privacy policies and requirements.

- USCIS developed a privacy newsletter on the importance of protecting privacy for Data Privacy Day that was distributed to the USCIS Directorates and Program Offices on January 28, 2023.

U.S. Coast Guard (USCG)

October 1, 2021 – March 31, 2022

- USCG provided instructor-led privacy training for 230 personnel.
- In this reporting period, 85 USCG employees completed operational use of social media training.
- USCG provided flyers highlighting requirements and instructions for encrypting electronic sensitive information. They were distributed to all Commands investigating confirmed or suspected privacy incidents as part of their privacy incident programs.
- USCG created privacy informational notices that were broadcast on television screens throughout the Coast Guard's Headquarters in Washington, DC.
- USCG expanded its privacy awareness campaign beyond USCG headquarters to become a service-wide campaign that includes publishing the information notices on the "Special notices" page on the Coast Guard Portal.
- USCG conducted an outreach activity through which a member of USCG Privacy attended the Assistant Commandant for C4IT (CG-6) Leadership and Diversity Advisory Council's March 2022 monthly meetings to discuss employee privacy obligations when collecting, accessing, sharing, and disposing of personally identifiable information. Emphasis was also placed on reporting all suspected and confirmed privacy incidents to Commanding Officers, the Office of Privacy Management, and CGCYBER Command.

April 1, 2022 – September 30, 2022

- USCG provided instructor-led privacy training to 170 personnel.
- In this reporting period, 71 USCG employees completed operational use of social media training.
- USCG provided flyers highlighting requirements and instructions for encrypting electronic sensitive information. They were distributed to all Commands investigating confirmed or suspected privacy incidents as part of their privacy incident programs.
- USCG created informational notices that were broadcast on television screens located throughout the Coast Guard Headquarters in Washington, DC.
- USCG expanded its privacy awareness campaign beyond USCG headquarters to become a service-wide campaign that includes publishing the information notices on the "Special notices" page on the Coast Guard Portal.

October 1, 2022 – March 31, 2023

- USCG Privacy presented new employee privacy awareness training to 170 employees at six bi-monthly USCG Civilian Employee Orientation sessions.
- In this reporting period, 70 USCG employees completed operational use of social media training.
- USCG provided flyers highlighting requirements and instructions for encrypting electronic sensitive information. They were distributed to all Commands investigating confirmed or suspected privacy incidents as part of their privacy incident programs.
- USCG created informational notices that were broadcast on television screens throughout the Coast Guard Headquarters in Washington, DC.
- USCG expanded its privacy awareness campaign beyond USCG headquarters to become a service-wide campaign that includes publishing the information notices on the "Special notices" page on the Coast Guard Portal.

- A Privacy Analyst routinely attended the Assistant Commandant for C4IT (CG-6) Leadership and Diversity Advisory Council's (LDAC) monthly meeting to advise the Council on DHS/USCG policy for safeguarding personally identifiable information collected through the LDAC's activities, including information regarding privacy compliance requirements, such as Privacy Threshold Analysis documents.

U.S. Customs and Border Protection (CBP)

October 1, 2021 – March 31, 2022

- CBP provided instructor-led privacy training to 593 personnel.
- In this reporting period, 639 CBP employees completed the *Operational Use of Social Media* training, and 41,091 employees completed *Personal Use of Social Media training*
- During the reporting period the CBP Privacy Office continued its proactive outreach and awareness campaign efforts, in addition to targeted training associated with incident response, to expand the 'privacy footprint' and develop a culture of awareness throughout the agency. Instructor-led training sessions were conducted virtually across the following program offices:
    - Management Inspections Division, Audit Team
    - Office of International Affairs, Overseas Support Branch
    - Office of Acquisitions Acquisition, Workforce and Knowledge Management Division
    - Office of Professional Responsibility, Threat Mitigation and Analysis Division
    - Office of Professional Responsibility, Credibility Assessment Division
    - Freedom of Information Act
    - Brownsville Port of Entry, U.S. Border Patrol
    - New York Fusion Office, Center for Intelligence, Targeting and Enforcement
    - Office of Trade, Textiles and Trade Agreements Division
    - Commercial Targeting and Analysis Center
    - Joint Terrorism Task Forces, New York Field Office
    - Human Capital, Operations Support
    - Houston Field Office, Office of Field Operations
    - Baltimore Field Office, Office of Field Operations
- During the reporting period, CBP Privacy began providing instructor-led training on 'Domestic Information Sharing for law enforcement and security purposes.' This training impacts 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 instructor-led training effort is designed to expand employee knowledge and understanding of the Directive. It was developed to remedy information sharing challenges and outline a streamlined domestic information sharing process. In addition to the training effort, and to accompany the Directive, CBP Privacy also developed an abridged training, available to all employees via the agency's Learning Management System.
- CBP Privacy began coordination efforts with the Office of Technology and Development to develop a thorough and substantive training course in the agency's Learning Management System on domestic and foreign information sharing for law enforcement and security.
- CBP Privacy continued to capitalize on the close partnership with the Office of Information Technology, Cyber Defense Forensics Team using collaborative efforts to contribute privacy equities to various IT-security messaging and aspects of the agency's data loss prevention tools.
- CBP Privacy is a standing participant in the CBP Office of Acquisitions' Annual Lunch & Learn training venue, designed to facilitate discussions of privacy inclusion in contract administration with

respect to Homeland Security Acquisition Regulation Class Deviation clauses and other privacy fundamentals.

- CBP continued to heighten personnel privacy awareness and responsibilities throughout the agency using the agency's Information Display System, main internal webpage (CBPnet), and other information delivery options. Messages are streamed monthly and include seasonal and holiday-themed communications.

April 1, 2022 – September 30, 2022

- CBP provided instructor-led privacy training for 2,254 employees.
- In this reporting period, 503 CBP employees completed CBP Training for the *Operational Use of Social Media,* and 21,511 employees completed the training course, *Personal Use of Social Media*.
- During the reporting period, the CBP Privacy Office remained constant in its customary proactive outreach and awareness efforts, including targeted training resulting from incident metrics. Additionally, the reporting period included the implementation and completion of the CBP Privacy virtual training initiative to support agency information sharing initiatives. The training focused on personnel involved in the sharing of information in support of activities conducted by an appropriate Domestic Federal, State, Local, or Tribal authority charged with investigating or prosecuting a violation, or enforcing or implementing a law, rule, regulation, or order; or in support of the protection or safety of the United States Government and/or CBP personnel, facilities, and/or operations. In addition, CBP Privacy developed an abridged version of the training presentation which is available to all employees via the agency's Learning Management System.
- CBP Privacy continued to capitalize on the close partnership with the Office of Information Technology, Cyber Defense Forensics Team using collaborative efforts to contribute to privacy equities to various IT-security messaging and certain aspects of the agency's data loss prevention tools.
- CBP Privacy is a standing participant in the CBP Office of Acquisitions' Annual Lunch & Learn training venue, designed to facilitate discussions of privacy inclusion in contract administration, with respect to Homeland Security Acquisitions Regulation Class Deviation clauses and other privacy fundamentals.
- Continued efforts to heighten personnel privacy awareness and responsibilities throughout the agency through broadcasted privacy messaging by utilizing the agency's Information Display System, main internal webpage (CBPnet), and other information delivery mechanisms. Messages were streamed monthly to include seasonal and holiday-themed messages.

October 1, 2022 – March 31, 2023

- CBP provided instructor-led privacy training for 783 personnel.
- In this reporting period, 39,134 CBP employees completed CBP Training for the *Operational Use of Social Media* and the training course, *Personal Use of Social Media*.
- During the reporting period, the CBP Privacy Office continued training and outreach efforts in support of the new Domestic Information Sharing Directive for Law Enforcement and Security Purposes (4320-033). This training focuses on personnel involved in the sharing of information in support of activities conducted by an appropriate Domestic Federal, State, Local, or Tribal authority charged with investigating or prosecuting a violation, or enforcing or implementing a law, rule, regulation, or order; or in support of the protection or safety of the United States Government and/or CBP personnel, facilities, and/or operations. The newly established Directive delegates much authority to the operational offices. The training helped to provide instructions 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. In addition,to accompany the CBP Privacy also developed an abridged training which is available to all employees via the agency's Learning Management System.

- CBP Privacy launched the development of training on the *Sharing of Information with Foreign Authorities*, which will support the recently updated Directive on Foreign Disclosures (4320-025B). Development of this training is projected for completion by the end of 2023.
- Because of its robust privacy incidents program and rigorous training & outreach efforts, CBP Privacy personnel mitigated hundreds of inquiries, including many information sharing inquiries and inquiries regarding agency policy/protocol pertaining to the safeguarding of personally identifiable information that is transmitted electronically (email). CBP Privacy also remained constant in its mitigation and remediation efforts in response to privacy incidents, including targeted refresher privacy training driven by incident metrics. Instructor-led training was conducted virtually and provided to various operational offices within the Office of Field Operations, Border Patrol, and other essential program offices**.**
- CBP Privacy continued to capitalize on the close partnership with the Office of Information Technology, Cyber Defense Forensics Team through collaborative efforts by contributing privacy equities to various IT-security messaging regarding the agency's data-loss prevention tools and collaborative tools and sites (e.g. – SharePoint).
- CBP Privacy is a standing participant in the CBP Office of Acquisitions' Annual Lunch & Learn training venue, designed to facilitate discussions about privacy in contract administration with respect to Homeland Security Acquisition Regulation Class Deviation clauses and other privacy fundamentals.
- CBP Privacy continued its efforts to heighten personnel privacy awareness and responsibilities throughout the agency through broadcasted privacy messaging by utilizing the agency's Information Display System, main internal webpage (CBPnet), and other streams of information delivery. Messages were streamed monthly to include seasonal and holiday-themed messages.

U.S. Immigration and Customs Enforcement (ICE)

October 1, 2021 – March 31, 2022

- ICE conducted the following privacy training:
    - Privacy Training for 100 ICE Information System Security Officers (ISSOs) on January 27, 2022.
    - Privacy Training for 89 Office of Homeland Security Investigations (HSI) Division 1 and Intel attendees in Texas on February 1, 2022.
    - Privacy Training for 77 HSI Division 2 and Division 3 attendees in Texas on February 2, 2022.
    - Privacy Training for 61 HSI Division 4 and Special Operations Group attendees in Texas on February 3, 2022.
    - Privacy Training for 84 HSI Division 6 attendees in Texas on February 4, 2022.
    - Privacy Training for 2 HSI Division 6 attendees in Texas on February 14, 2022.
    - Training for 101 ICE Mission Support staff regarding Privacy and Freedom of Information Act policies and compliance requirements on February 15, 2022.
    - Privacy and Media Release Training for 32 ICE Office of Public Affairs employees on March 22, 2022.

April 1, 2022 – September 30, 2022

- ICE conducted the following privacy training:

- New Employee Onboarding Privacy Awareness training on May 4, 2022.
- Privacy Awareness training for 37 ICE Mission Support staff on April 26, 2022.
- Procurement Training for 175 ICE Contracting Official Representatives on May 12, 2022.
- Privacy Awareness training for 41 ICE Mission Support staff on June 28, 2022.
- New Employee Onboarding Privacy Awareness training on July 5, 2022.

U.S. Secret Service (USSS)

October 1, 2021 – March 31, 2022

- During the week of January 28, 2021, the USSS created and posted a Privacy Awareness Poster and fact sheet to USSS intranet to enhance privacy awareness.
- USSS trained 176 new employees virtually on privacy during New Employee Orientation.
- USSS provided instructor-led privacy training courses for 156 personnel.
- In this reporting period, 2,936 USSS staff members completed operational use of social media training.

April 1, 2022 – September 30, 2022

- USSS trained 398 new employees virtually on privacy during New Employee Orientation.
- USSS provided instructor-led privacy training courses for 349 personnel.
- In this reporting period, 376 USSS staff members completed operational use of social media training.

October 1, 2022 – March 31, 2023

- USSS trained 176 new employees virtually on privacy during New Employee Orientation.
- USSS provided instructor-led privacy training courses for 236 personnel.
- In this reporting period, 13 USSS staff members completed operational use of social media training.

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 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 do not pertain to Privacy Act matters.
    a. *Example:* An individual alleges that personal health information was disclosed to a non-supervisor.
    b. *Example:* An individual alleges that physical screening and pat-down procedures at airports violate their privacy rights.
4. ***Referred*:** Complaints referred to another federal agency or external entity for handling.
    a. *Example:* A member of the public submits an inquiry regarding the individual's driver's license or Social Security number.

The DHS Privacy Office reviews redress complaints received by the DHS Traveler Redress Inquiry Program (DHS TRIP) that may have a privacy nexus. DHS TRIP is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs—like airports—or crossing U.S. borders. This includes watchlist issues, screening problems at ports of entry, and situations 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, 647 travelers marked that box. Upon review, none of the complaints received through TRIP described a privacy violation.

October 1, 2021 – March 31, 2022

During the reporting period, the Department received **1,260** privacy complaints outside of the TRIP process.

Type	CBP	CISA	FEMA	FPS	FLETC	ICE	TSA	USCIS	USCG	USSS	TOTAL
Procedure	465	0	0	0	0	0	0	0	0	0	**465**
Redress	0	0	0	0	0	0	0	0	0	0	**0**
Operational	769	0	0	0	0	0	26	0	0	0	**795**
Referred	0	0	0	0	0	0	0	0	0	0	**0**

TOTALS	**1,234**	**0**	**0**	**0**	**0**	**0**	**26**	**0**	**0**	**0**	**1,260**

Procedural and Operational Examples

Procedural

- The Complainant reported that items were insufficiently resealed after CBP inspection and that items were subsequently damaged during transit. The case was transferred to the CBP field office invovled for review and follow-up.
- The Complainant reported they were held in a detention center by CBP for 17 hours in the Los Angeles International Airport before being sent on a flight back to Australia. The case was transferred to the CBP field office involved for review and follow up.
- The Complainant appealed the revocation of their status in the Trusted Traveler Program for issuance of an Agriculture violation with a penalty by CBP. The case was transferred to the CBP field office involved for review and follow-up.

Operational

- The Complainant reported a CBP officer pushed them and that the officer snapped his finger at the Complainant. The case was transferred to the CBP field office involved for review and follow-up.
- The Complainant reported a CBP agent was rude and condescending when providing information to and questioning the Complainant's family. The Complainant also reported the agent incorrectly insisted children under the age of 15 in the car needed a passport. CBP requested additional information regarding the incident to address the complaint, which was not provided.
- A TSA employee complained that their privacy rights were violated by an agency policy requiring unvaccinated employees to wear a face shield at airport checkpoints. TSA Privacy advised that the policy did not violate any privacy policies, noting that all employees were permitted to choose to wear a face shield so that employees with face shields did not necessarily indicate that they were unvaccinated.

April 1, 2022 – September 30, 2022

During the reporting period, the Department received **454** privacy complaints outside of the TRIP process.

Type	CBP	CISA	FEMA	FPS	FLETC	ICE	TSA	USCIS	USCG	USSS	TOTAL
Procedure	83	0	0	0	0	0	2	1	0	0	**86**
Redress	0	0	0	0	0	0	0	0	0	0	**0**
Operational	338	0	0	0	0	3	27	0	0	0	**368**
Referred	0	0	0	0	0	0	0	0	0	0	**0**
TOTALS	**421**	**0**	**0**	**0**	**0**	**3**	**29**	**1**	**0**	**0**	**454**

Procedural and Operational Examples

Procedural

- The Complainant reported a CBP agent took a picture of the Complainant's passport ID page using the agent's personal cell phone. The case was transferred to the CBP field office involved for review and follow up.
- The Complainant called CBP to inquire when they could retrieve a car detained by U.S. Border Patrol because it was suspected of use for transporting undocumented immigrants. The caller was informed that the car is now part of an investigation and that they will be contacted about the vehicle most likely when the case is closed.
- A USCIS employee complained that their supervisor sent an email containing a written letter of counseling that was visible and accessible to their co-workers who did not have a need to know, and the supervisor failed to properly secure the information in accordance with agency policies and procedures, which allegedly violated his privacy rights. The employee no longer works for the agency, and due to its inability to contact the employee to validate the complaint, USCIS closed the complaint and recorded the findings.

Operational

- The Complainant reported that their personally identifiable information, including name, date of birth, and passport number was available in a Freedom of Information Act (FOIA) log posted on the CBP FOIA reading room. The case was transferred to the CBP Privacy and Diversity Office (FOIA) for review and follow-up.
- The Complainant reported a CBP officer threatened to revoke their Global Entry membership for refusing to answer personal questions in front of several people. The case was transferred to the CBP field office involved for review and follow-up.
- The Complainant reported that they could not opt-out of biometric identification at an airport and that their photo was shared with private sector social media companies. TSA Privacy noted that the flight was more than a month prior but that it is the policy for signage to be in place and confirmed that signs are present at that airport. The photograph taken of the passenger is checked against the photo scanned from the driver's license and then deleted. Scans are not shared with any private sector companies.
- The Complainant alleged that an ICE employee violated their privacy and civil rights when the employee printed out the individual's personal and confidential information and provided the information to other individuals for civil court matters. The information shared is not available in public records. ICE Privacy reviewed the complaint and after searching ICE Active Directory, the violator in question is not an active ICE employee. A follow-up email was sent to the Complainant for additional information about the violator, but a response was never received. The complaint was then closed.
- The Complainant alleged that an ICE employee is using their credentials to perform background checks on the Complainant and the Complainant's family members. The individual has not applied to any government position that would warrant a background check, nor has their family members. The individual claimed that the ICE employee was misusing their position to query information on the individual's license plate, thus acquiring personal information on the individual's address and work location. ICE Privacy reviewed the complaint and determined that it required further investigation and intervention from the ICE Office of Professional Responsibility (OPR), Investigations Program Office. Due to the Privacy Act and Agency

Privacy Policy, OPR is not permitted to provide the status, the entity conducting the inquiry, and/or the final disposition of allegations and/or complaints received.

- The Complainant alleged that their company was selected for an ICE audit, during which they presented their employees' I-9 forms, payroll reports, and tax documentation to ICE agents when the agents arrived at their office. However, the aforementioned documents were never returned to the company. After a thorough investigation, ICE Privacy confirmed that the ICE Office of Homeland Security Investigations (HSI) is still in possession of the employees' documentation because the audit is ongoing. The documents will be returned after the audit is completed. ICE Privacy sent a response letter to the Complainant informing them of the results of its investigation.

October 1, 2022 – March 31, 2023

During the reporting period, the Department received 46 privacy complaints outside of the TRIP process.

Type	CBP	CISA	FEMA	FPS	FLETC	ICE	TSA	USCIS	USCG	USSS	TOTAL
Procedure	5	0	0	0	0	0	4	1	0	0	**10**
Redress	0	0	0	0	0	0	0	0	0	0	**0**
Operational	11	0	0	0	0	0	25	0	0	0	**36**
Referred	0	0	0	0	0	0	0	0	0	0	**0**
TOTALS	**16**	**0**	**0**	**0**	**0**	**0**	**29**	**1**	**0**	**0**	**46**

Procedural and Operational Examples

Procedural

- The Complainant reported that a CBP agent reviewed personal information, including their Facebook page and bank account because the agent suspected they were in a relationship with someone in the United States. Because the complaint was submitted anonymously, it was categorized for topic, location, and privacy, then closed.
- The Complainants reported their passports were given to the wrong individuals by CBP after agriculture screening. Because the complaint was submitted anonymously, it was categorized for topic, location, and privacy, then closed.
- A USCIS employee alleged that their right to privacy was violated when a Reasonable Accommodations Point of Contact inappropriately shared medical information with their immediate Supervisor. During the initial stage of the investigation, the employee requested to withdraw the complaint. The complaint was withdrawn and officially closed.

Operational

- The Complainant, a U.S. citizen, reported that an agent asked personal questions and humiliated them before detaining them with no explanation. The Complainant was provided information on how to file a Traveler Redress Inquiry.
- The Complainant alleged that a TSA complaint form lacked a Privacy Act notice and that a web application available to print complaints appeared to send data to a private-sector company. The Privacy Office determined that the Privacy Act notice was properly available to the Complainant prior to preparing the complaint form, and that while the private-sector application did not

collect Complaint information, it should nevertheless be eliminated from the website to avoid confusion and to use other print existing capabilities. Removal was accomplished within two days.

APPENDIX A– PUBLISHED PRIVACY IMPACT ASSESSMENTS

Privacy Impact Assessments Published October 1, 2021 – March 31, 2023	
DHS Component and System Name	**Date Published**
DHS/CBP/PIA-017(a) Non-Intrusive Inspection Systems Program: Pedestrian Detection-at-Range	10/6/2021
DHS/CBP/PIA-016(b) I-94 Website Application	10/15/2021
DHS/ICE/PIA-060 ICE Pilot on Use of Body Worn Cameras	11/3/2021
DHS/USCIS/PIA-044(b) Validation Instrument for Business Enterprises (VIBE)	11/19/2021
DHS/TSA/PIA-050 Amtrak Rail Passenger Threat Assessment	12/1/2021
DHS/CBP/PIA-013(a) Customs Trade Partnership Against Terrorism (C-TPAT)	1/5/2022
DHS/TSA/PIA-019(c) Air Cargo Program	1/5/2022
DHS/TSA/PIA-051 Travel Document Checker Automation- Digital Identity Technology Pilots	1/18/2022
DHS/ICE/PIA-061 Homeland Security Investigation (HSI) Surveillance Technologies	1/24/2022
DHS/USCIS/PIA-086 Employee Production Reporting Tools (EPRT)	2/1/2022
DHS/ICE/PIA-046(a) Laboratory Information Management System	2/2/2022
DHS/ALL/PIA-092 Immigrant Military Members and Veterans Initiative (IMMVI)	2/7/2022
DHS/S&T/PIA-043 Operations and Requirements Analysis Division	2/10/2022
DHS/S&T/PIA-042 DHS Federally Funded Research and Development Centers (FFRDC)	2/22/2022
DHS/USCIS/PIA-080(a) Enterprise Gateway and Integration Services (EGIS)	3/18/2022
DHS/CBP/PIA-072 Unified Immigration Portal (UIP)	4/7/2022
DHS/ALL/PIA-093 Hummingbird	4/28/2022
DHS/OBIM/PIA-005 Office of Biometric Identity Management (OBIM)-National Institute of Standards of Technology (NIST) Data Transfer	5/16/2022
DHS/TSA/PIA-052 Checkpoint Information Management (CIM) Web Application	5/16/2022
DHS/ALL/PIA-094 Migrant Protection Protocols (MPP) Case Request System	5/20/2022
DHS/FEMA/PIA-056 Administered Disaster Case Management Program	5/27/2022

Privacy Impact Assessments Published October 1, 2021 – March 31, 2023	
DHS Component and System Name	**Date Published**
DHS/USCIS/PIA-057(b) National Appointment Scheduling System (NASS)	6/17/2022
DHS/OBIM/PIA-006 Automated Real-Time Identity Exchange System (ARIES)	7/18/2022
DHS/USCG/PIA-028(a) Defense Sexual Assault Incident Database (DSAID)	7/29/2022
DHS/ALL/PIA-048(c) Foreign Access Management System (FAMS)	8/18/2022
DHS/CBP/PIA-063 CBP Enterprise Analytics	9/6/2022
DHS/CBP/PIA-073 Advance Travel Authorization	10/17/2022
DHS/CBP/PIA-074 CBP Personnel Recovery Program	10/26/2022
DHS/ALL/PIA-095 International Biometric Information Sharing (IBIS) Program	11/02/2022
DHS/CBP/PIA-075 Intelligent Computer Assisted Detection (ICAD) System	11/4/2022
DHS/TSA/PIA-046(d) Travel Document Checker Automation Using Facial Identification	11/17/2022
DHS/ALL/PIA-095(a) International Biometric Information Sharing (IBIS) Program	11/18/2022
DHS/TSA/PIA-029(b) TSA Operations Center Information Management System	12/6/2022
DHS/USCIS/PIA-087 Person Centric Identity Services (PCIS) Initiative	12/7/2022
DHS/ALL/PIA-096 Employment Verification and Unemployment Compensation (EV UC)	1/11/2023
DHS/USCIS/PIA-062(a) Administrative Appeals Office Case Management System	1/30/2023
DHS/ALL/PIA-046 DHS Data Framework	3/21/2023
DHS/USCG/PIA-032 SURVEYOR Integrated Data Environment (IDE)	3/27/2023

APPENDIX B – PUBLISHED SYSTEM OF RECORDS NOTICES

System of Record Notices Published October 1, 2021 – March 31, 2023	
DHS Component and System Name	**Date Published**
DHS/CBP-025 CBP Recruitment and Hiring System of Records	11/15/2021
DHS/FEMA-016 Disaster Case Management (DCM) Files System of Records	11/15/2021
DHS/ICE-005 Trade Transparency Analysis and Research	12/29/2021
DHS/FEMA-008 Disaster Recovery Assistance Files	1/3/2022
DHS/CBP-014 Regulatory Audit Archive System (RAAS)	1/27/2022
DHS/ALL-033 Reasonable Accommodations Records System of Records	3/17/2022
DHS/FEMA-004 Non-Disaster Grant Management Information Files	6/9/2022
DHS/CBP-009 Electronic System for Travel Authorization (ESTA)	6/9/2022
DHS/CBP-027 Customs Broker Management	6/9/2022
DHS/CBP-027 Customs Broker Management Final Rule	7/22/2022
DHS/FEMA-017 Individuals and Households Program Equity Analysis Records System of Records	7/26/2022
DHS/FEMA-012 Suspicious Activity Reporting System of Records	1/24/2023