Privacy Office

FY 2021 Annual Report to Congress

October 2022

Homeland Security

Message from the Chief Privacy Officer

It is my great pleasure to deliver my first Annual Report of the DHS Privacy Office as the Department of Homeland Security (DHS) Chief Privacy Officer.

I am immensely proud of the Privacy Office's contributions to the Department's work. The Privacy Office offers valuable insight into potential privacy risks and offers actionable suggestions for how to mitigate these risks while accomplishing the Department's mission. The Privacy Office works in close collaboration with component privacy officers and fellow privacy professionals across the Department to ensure privacy protections are embedded into the Department's activities.

Privacy is an ever-evolving field, and its incumbent on privacy professionals to keep up with the rapid advances in technologies and to understand how the availability and sharing of data impacts privacy. In addition to identifying and mitigating risks, I see a huge opportunity for privacy professionals to understand and encourage the use of privacy enhancing technologies.

One of my priorities as the DHS Chief Privacy Officer is to integrate privacy into the Department's strategic architecture. With input and advice from technologists, researchers, advocates, and others, the DHS Privacy Office continues to educate the workforce on the benefits of privacy tools and encourage early program integration. This work will only enhance the Privacy Office's service to the Department and the public while instilling trust in Department operations.

Please direct any inquiries about this report to the DHS Office of Legislative Affairs at 202-447-5890 or privacy@dhs.gov.

Sincerely,

Lynn Parker Dupree

Lynn Parker Dupree
Chief Privacy Officer and Chief FOIA Officer
U.S. Department of Homeland Security

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 Rob Portman
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Dick Durbin
Chairman, Senate Committee on the Judiciary

The Honorable Chuck Grassley
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 Bennie G. Thompson
Chairman, House Committee on Homeland Security

The Honorable John Katko
Ranking Member, House Committee on Homeland Security

The Honorable Carolyn Maloney
Chairwoman, House Committee on Oversight and Reform

The Honorable James Comer
Ranking Member, House Committee on Oversight and Reform

The Honorable Jerrold Nadler
Chair, House Committee on the Judiciary

The Honorable Jim Jordan
Ranking Member, House Committee on the Judiciary

The Honorable Adam Schiff
Chairman, House Permanent Select Committee on Intelligence

The Honorable Michael Turner
Ranking Member, House Permanent Select Committee on Intelligence

DHS Privacy Office
FY 2021 Annual Report to Congress
Table of Contents

Contents

Executive Summary

While this report is focused on activities in Fiscal Year (FY) 2021, the report also provides an overview of work since the Privacy Office published its last report, which covered the period of July 1, 2018 – June 30, 2019. With the publication of this report, the Privacy Office will begin submitting its Annual Report to coincide with each Fiscal Year.

This report highlights the Privacy Office's work to provide privacy advice and oversight of the Department's programs. The Privacy Office enables the Department to accomplish its mission while embedding and enforcing privacy protections and transparency in all DHS activities. All DHS systems, technology, forms, and programs that collect personally identifiable information or have a privacy impact are subject to the oversight of the Chief Privacy Officer and the requirements of U.S. data privacy and disclosure laws.

In FY 2021 the Chief Privacy Officer placed a special emphasis on identifying and encouraging the use of privacy enhancing technologies. Specifically, the Privacy Office has worked in partnership with the Science and Technology Directorate (S&T) Silicon Valley Innovation Program (SVIP) on the use of decentralized identifiers as a replacement for a Social Security Number (SSN) in DHS systems. This technology can improve privacy protections and reduce individual risk. The Privacy Office also identified other cases where a decentralized identifier might be beneficial. These cases include comparing separate decentralized identifiers to confirm a person's identity without sharing a social security number and replacing other potentially sensitive data elements.

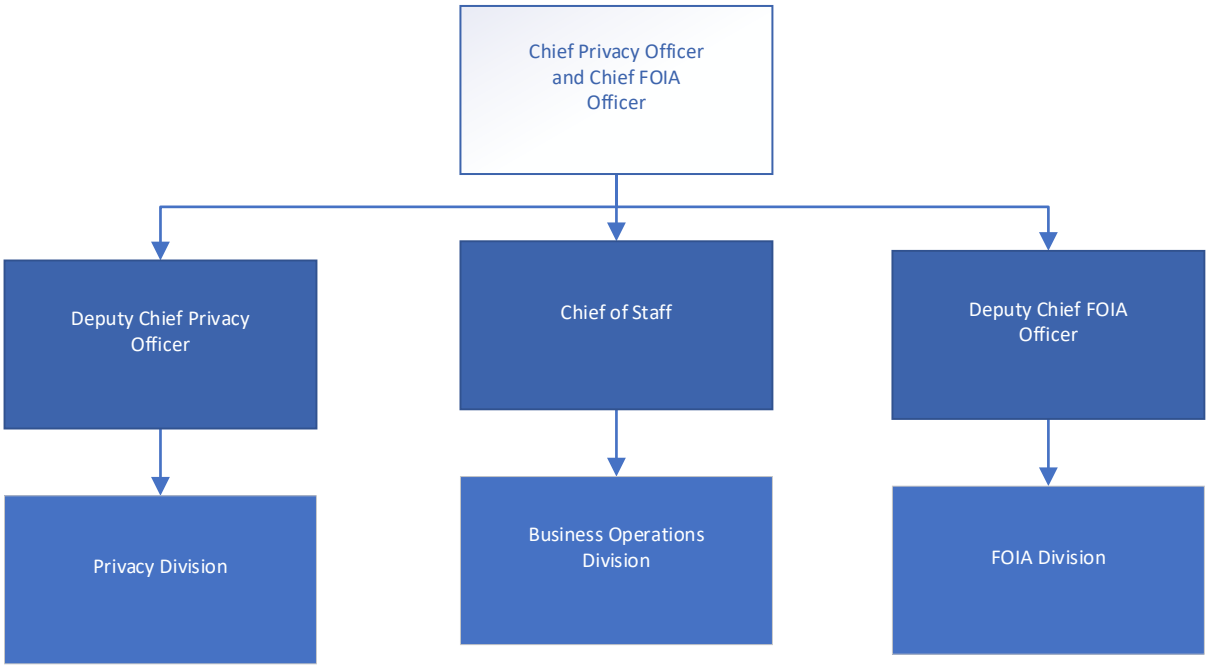
Additionally, the report provides an update on the Privacy Office's work on cross-cutting and emerging issues, including the use of biometrics, the deployment of artificial intelligence (AI) and machine learning (ML), and the response to the global pandemic. The Privacy Office is deeply engaged in addressing these issues in partnership with components throughout the Department and relies both on the compliance documentation process and continuous engagement in the Department's policymaking process to ensure privacy risks are identified and mitigated.

This report provides updates regarding policy engagements that impact privacy and compliance program operations. Additionally, the report covers the Privacy Office's oversight activities, including use of Privacy Compliance Reviews, privacy investigations, and response to privacy breaches and complaints.

The report also includes information about the Privacy Office's work to engage the broader privacy community, including through its federal advisory committee, the Data Privacy and Integrity Advisory Committee (DPIAC) that provides privacy education, through training and other fora. Finally, the report provides insight into activities of the business operations team ensuring the efficiency of office operations, as well as the development and execution of internal and external communication strategies.

Organization

The DHS Privacy Office is composed of three divisions: the Privacy Division, the Freedom of Information Act (FOIA) Division, and the Business Operations Division. Each of these divisions is critical to ensuring that privacy and transparency are integrated into the Department's mission.



The Privacy Division collaborates with Privacy Officers appointed at ten components,[1] as well as privacy points of contact (PPOC)[2] and program offices on the development of policy and preparation of compliance documentation. Highlights of component privacy office accomplishments are detailed in Semi-Annual Section 803 Reports.

DHS Privacy Office	Component Privacy Officers	Privacy Point of Contact
• Privacy Policy and Oversight Team • Privacy Compliance Team	• Cybersecurity and Infrastructure Security Agency (CISA) • Federal Emergency Management Agency (FEMA)	• Countering Weapons of Mass Destruction Office (CWMD) • Office of the Chief Human Capital Officer (OCHCO)

[1] Every DHS component is required by DHS policy 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.

[2] PPOCs 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, PPOCs work closely with component program managers and the Privacy Office to manage privacy matters within DHS.

DHS Privacy Office	Component Privacy Officers	Privacy Point of Contact
	• 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 (Coast Guard) • U.S. Customs and Border Protection (CBP) • U.S. Immigration and Customs Enforcement (ICE) • U.S. Secret Service (Secret Service) • Office of Biometric Identity Management (OBIM) • Office of Inspector General (OIG) • Federal Law Enforcement Training Centers (FLETC) • National Vetting Center (NVC)	• Office of the Citizenship and Immigration Services Ombudsman (CISOMB) • Office of Operations Coordination (OPS) • Office of Public Affairs (OPA)

I. Privacy Enhancing Research and Development

The DHS Privacy Office recognizes valuable potential in the development and integration of privacy enhancing technologies into Department operations and is taking steps to become a proactive partner in identifying and encouraging development and use of these emerging technologies. Integrating privacy enhancing technology into the Department's strategic architecture offers several benefits. In addition to improving privacy protections privacy enhancing technology can make privacy-conscious decisions the default rather than an option, thereby increasing consistent application of privacy protections. This work is a natural complement and force-multiplier to our robust compliance governance work of evaluating privacy risks in technology and suggesting methods to mitigate those risks.

The Privacy Office's current work in this area is an outgrowth of a privacy policy requiring all new and legacy IT systems, programs, and forms to use a unique alternate identifier to SSNs. The policy states that if there are technological, legal, or regulatory limitations to eliminating the use of SSNs, then privacy enhancing SSN alternatives must be utilized, such as masking, redacting, or truncating SSNs in digital and hard copy formats.

To assist components with reducing SSN use while better protecting privacy, the Privacy Office partnered with the S&T SVIP to explore replacing SSNs or other personal identifiers with decentralized identifiers. Through this work, the Privacy Office recognized the value privacy enhancing technologies may have in other contexts. As a result, the Privacy Office participated in other opportunities to learn more about ongoing research in this area and offered DHS components access as well.

In June 2022, the Privacy Office held a workshop in conjunction with S&T's Center for Accelerating Operational Efficiency, led by Arizona State University, that brought together academia and researchers to discuss DHS specific use cases that may be solved with privacy enhancing technologies. The Privacy Office conducted a Department-wide call for potential issues that could be addressed through the implementation of privacy enhancing technologies and gave each component the opportunity to speak about its specific goals. Academic researchers presented their work and informed DHS officials about privacy technology use when developing programs and systems. As a result of the workshop, researchers are able to submit proposals to the National Science Foundation for projects that support DHS specific operational and privacy requirements. The Privacy Office will track the number of potential use cases accepted for research, the development of research plans, and timelines for deliverables.

II. Cross-Cutting and Emerging Issues

Privacy is ever evolving, and protecting it is critical to meet the Department's mission as programs and technology change. Building privacy into operations relies on active engagement. The Privacy Office accomplishes this work through policymaking and compliance documentation.

Artificial Intelligence

The Privacy Office is operationalizing privacy risk assessment and mitigation at DHS for artificial intelligence and machine learning (AI/ML) technology by:

- including specific questions on the Privacy Threshold Analysis (PTA) template covering Data Mining Reporting for applicable technology, systems or programs that leverage PII.
- assessing privacy risks of and mitigations for AI/ML technology identified through the privacy compliance process, PTAs, Privacy Impact Assessments (PIAs), and System of Records Notices (SORNs).
- participating in Departmental and external working groups, including the federal Artificial Intelligence Community of Interest, and the DHS Artificial Intelligence Implementation Plan Working Group, which is developing targeted recommendations for the goals and objectives of the DHS Artificial Intelligence Strategy.
- ensuring inclusion of appropriate safeguards in information sharing access agreements (ISAAs) with external partners; and
- ensuring that AI/ML projects adhere to existing governance procedures.

The Privacy Office is also taking part in various discussions at the interagency level and with the public regarding the impact to privacy when leveraging AI/ML technology by:

- gathering civil society and private sector input and insight on effects to the individual as well as unintended consequences that may arise from the use of AI/ML; and
- sharing best practices.

Biometrics

The Privacy Office ensures the Fair Information Privacy Practices (FIPPs) are applied to the Department's collection, maintenance, and use of biometric data, especially to the challenges inherent to data quality and integrity when using biometrics. This is accomplished by leveraging prior Privacy Office recommendations in Privacy Compliance Reviews and PIAs, as well as accountability requirements in information sharing agreements for additional procedures and documentation to ensure data quality and integrity satisfy operational requirements while upholding privacy protections.

Biometric Information Sharing and Identity Verification

Biometrics-based information sharing is rapidly increasing across the DHS enterprise as technology advances to support identity verification and investigations —such as when sexual exploitation of children is suspected— through facial recognition and other modalities, in addition to manual examination of photos and traditional fingerprint matching. During the reporting period, the Privacy Office provided privacy guidance in the negotiation and implementation of biometric interoperability agreements with the Departments of Justice and Defense and has helped resolve privacy issues related to international biometric information sharing.

Biometric-based enterprise information sharing of multiple modalities becomes more complex as new modalities, new uses, and new users are brought online. Privacy analysis must, in part, consider variables that can affect data quality and integrity because they are intrinsic to biometric match performance. In October 2019, the Privacy Office partnered with the S&T's Biometric and Identity Technology Center to train DHS privacy professionals on how biometric matching accuracy may be affected, tested, and documented for program-specific and enterprise information sharing purposes. Throughout the reporting period, Privacy Office staff joined several Departmental working groups on biometrics, including those focused on the collection of fingerprint, face, and iris scans. Several biometrics related PIAs published during the reporting period provide identification and analysis of novel privacy risks and mitigations.

Pandemic Preparedness

Throughout the reporting period, the Privacy Office worked diligently to ensure the Department identified and mitigated privacy risks associated with COVID-19 response activities and workforce protection measures.[3] Further, the Privacy Office remains involved within DHS and the interagency regarding policy development efforts connected to digital contact tracing, thermal imaging, and travel safety measures.

Specific initiatives include:

- **Temperature screening.** After numerous conversations with legal counsel and other stakeholders, DHS began temperature testing employees and visitors to DHS facilities using a non-contact temperature device. This was achieved without collecting PII, and facilities provided a privacy notice at the time of temperature reading.
- **Tracking workforce accountability.** DHS provided components guidance on how to implement measures for tracking individual cases for workforce accountability and resources while minimizing PII collection. DHS-wide guidance continues to evolve as the situation develops.

[3] Some of these initiatives are no longer in place.

- **Contact tracing**. DHS engaged in manual contact tracing efforts to ensure the safety of its workforce during this critical time. At the macro level, working closely with the Office of the Chief Human Capital Officer (OCHCO), the Privacy Office helped to develop DHS-wide contact tracing guidance. The Privacy Office collaborated with several components on the implementation of contact tracing methods to ensure privacy protections are sustained and not eroded, for each individual implementation.
- **Vaccinating frontline employees**. The Privacy Office continues to work with the DHS Vaccination Task Force (known as Operation Vaccinate Our Workforce—OVOW) to ensure protected health information of DHS employees is not compromised when voluntarily receiving inoculations through a partnership with the Veterans Health Administration (VHA). Privacy Office staff revised agreements between DHS and VHA to minimize the exchange of PII and protected health information between the two agencies, ensuring data is exchanged in a secure manner and collection and exchange of PII and protected health information is consistent with DHS policy and covered by required privacy compliance documentation.
- **Vaccination Status System (VSS)**. Pursuant to Executive Order 14043 - Requiring Coronavirus Disease 2019 Vaccination for Federal Employees (and prior to the injunction issuance), all DHS federal employees were to be fully vaccinated to promote the health and safety of the federal workforce and efficiency of the civil service unless they received or requested an exemption for religious or medical reasons (i.e., Reasonable Accommodation). All federal employees, including those who sought an exemption from the vaccination requirement for religious or medical reasons, were required to complete and submit their vaccination status via the VSS. This included the status itself, and proof of vaccination containing all required data elements into the system. The Privacy Office worked extensively with appropriate stakeholders to ensure appropriate privacy protections, such as access restrictions, were instituted regarding the collection and use of the data within the VSS.

III. Privacy and Disclosure Policy

Privacy Policy

Revised Privacy Policies

During the reporting period, the Privacy Office actively engaged component privacy officers and privacy points of contact in headquarters offices to develop operationally focused privacy directives and instructions, collectively considered privacy policy. Notably, the work on the DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (also known as the Mixed Systems Policy) was initiated during the reporting period and was finalized in May 2022. Additionally, three new directives and instructions were drafted and are currently under review before publication.

Acquisition Regulations and Departmental Policies

The Privacy Office continues to be involved in interagency Federal Acquisition Regulation (FAR) efforts. During the reporting period, the Privacy Office trained all Office of the Chief Procurement Officer senior staff on how to embed privacy protections into contracts.

Cybersecurity

The Privacy Office and the Office for Civil Rights and Civil Liberties (CRCL) assess the privacy and civil liberties impacts of the Departments' activities pursuant to two Executive Orders. These assessments are published annually in *Executive Order 13636/13691 Privacy and Civil Liberties Assessments Report*,[4] a report compiled by the Privacy Office and CRCL.

Fusion Centers

The Privacy Office established and continues to develop a robust privacy protection framework within the fusion center program, both at the national and state levels. The Privacy Office reviews all fusion center privacy policies to ensure they are as comprehensive as the Information Sharing Environment Privacy Guidelines and assists fusion centers with incorporating privacy protections in new policies and templates, such as facial recognition and automated license plate readers. The Privacy Office also collaborates with CRCL, I&A, and the Office of Partnership and Engagement to train fusion center privacy officers and analytical staff.

Joint Requirements Council

The Privacy Office supports the Joint Requirements Council (JRC), which reports to the Deputy Secretary's Management Action Group (DMAG). The JRC serves as an executive-level body to

[4] Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11737 (Feb. 19, 2013); Exec. Order No. 13691, Promoting Private Sector Cybersecurity Information Sharing, 80 Fed. Reg. 9347 (Feb. 20, 2015).

provide oversight of DHS operational requirements generation process, harmonize efforts across the Department, and make prioritized funding recommendations to the DMAG for those validated operational requirements. The JRC is also responsible for examining what tools and resources the Department needs to operate across a wide variety of mission areas including: aviation fleet; screening and vetting; information sharing systems; chemical, biological, radiological, and nuclear detection; and cybersecurity. The Chief Privacy Officer and the Deputy Chief Privacy Officer participate in the DMAG, as needed.

During the reporting period, the JRC set up a Countering Terrorism & Homeland Security Threats (CTHST) Portfolio Team (PT) to think strategically and horizontally about challenges across the Department to protect and defend the homeland in a future (3-5 years) operating environment. The Privacy Office supported the CTHST by reviewing and providing input to proposals for initiatives involving Countering Unmanned Aircraft Systems (C-UAS) and biometrics.

Unmanned Aircraft Systems

As outlined below, the Privacy Office plays a role in developing and publishing Unmanned Aircraft Systems (UAS) privacy compliance documentation; promoting transparency to support public understanding of the Department's use of UAS; ensuring the DHS UAS policy addresses rights and considerations; reviewing grant proposals from state, local, tribal, and territorial (SLTT) agencies that seek to acquire small UAS (sUAS); and developing policies and procedures to help counter threats to the Homeland from the use of UAS by our adversaries (Counter-UAS, or C-UAS).

Activity	Privacy Office Role	Reporting Period Update
Acquisition, development, or deployment of UAS by components	Review PTAs to determine potential privacy impacts. If any UAS operation or the use of C-UAS technology may result in DHS acquiring PII, the Privacy Office also requires a PIA.	Published: Science and Technology Directorate in 2012 and 2018 (updated in 2020); the U.S. Secret Service (USSS) in 2017, 2019, and 2020; United States Coast Guard in 2019; and the Federal Emergency Management Agency (FEMA) in 2020.
Acquisition of UAS using FEMA-administered preparedness grant funding by SLTT	Coordinate with CRCL to evaluate SLTT requests.[5]	Reviewed approximately thirty such requests during the reporting period.

[5] Presidential Document, Exec. Office of the President, Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, 80 Fed. Reg. 9355 (Feb. 20, 2015).

Violence Against Women Act

The Privacy Office and CRCL share responsibilities under Title 8, United States Code, Section 1367, *Violence Against Women Act* (VAWA) (herein Section 1367) related to incidents of unauthorized disclosures of information of non-citizen victims of crimes protected under the act. During the reporting period, the Privacy Office hosted three quarterly VAWA meetings with CRCL and components that work with special protected classes: CBP, ICE, OBIM, and USCIS. Additionally, the Privacy Office hosted one Special Protected Classes Unauthorized Disclosure Forum to refresh and educate the privacy points of contact and privacy incident practitioners. Section 1367 incident reporting has increased, which is a positive indicator that the Department-wide outreach is effective.

The Chief Privacy Officer also reviewed relevant PIAs and ISAAs to ensure the inclusion of language to protect Section 1367 records. The Privacy Office's FOIA Division also issued an instruction to FOIA professionals that outlines the requirement to withhold this information under applicable FOIA Exemptions and the requirement for annual training and notification to the Chief Privacy Officer of unauthorized disclosures made under FOIA.

Information Sharing and Intelligence Activities

The Privacy Office provides specialized expertise on ISAAs and programs to support the Department's information sharing activities with other federal agencies, the Intelligence Community (IC), state and local entities, and international partners.

There are currently more than 200 ISAAs governing how DHS shares information. Requests for new agreements or amendments to existing agreements continue at a rapid pace. The Privacy Office evaluates sharing requests that involve PII to mitigate privacy risks, incorporates privacy protections consistent with the Fair Information Practice Principles, and audits or otherwise measures the effectiveness of those protections over time.

Data Access Review Council

The Data Access Review Council (DARC) is the coordinated oversight and compliance mechanism to review departmental initiatives involving the internal or external transfer of PII through bulk data transfers that support the Department's national and homeland security missions. The DARC advises on challenges relating to bulk information sharing, including sharing in the cloud environment and application of advanced analytical tools to DHS data. The DARC ensures such transfers comply with applicable law and adequately protect the privacy, civil rights, and civil liberties of the individuals whose information is shared. As a discretionary matter, with the concurrence of other members, the DARC may also review any matter referred by a member concerning the internal or external transfer of data or the development, execution, implementation, or operation of any departmental information system.

DARC initiatives primarily involve ISAAs with members of the Intelligence Community. DARC membership includes the Privacy Office, I&A, the Office of Strategy, Policy and Plans (PLCY), the Office of General Counsel (OGC), and CRCL.

During the reporting period, the Privacy Office worked with DHS stakeholders and IC partners to approve six ISAAs or extensions for existing arrangements, and to ensure identification and mitigation of privacy risks by completing privacy compliance documentation for these agreements. The Privacy Office also monitors reports generated in accordance with existing agreements' provisions to ensure general adherence to the terms and to ensure appropriate reporting and mitigation of any privacy incidents involving DHS data.

Data Governance Council

DHS established the Data Governance Council (DGC) under the delegated authority from the Secretary to the DHS Chief Data Officer (CDO). The Council's purpose is to strengthen the management and oversight of enterprise data to support DHS components' effective and efficient mission delivery, advance integrated analytic capabilities, reduce duplicate data, and facilitate data-informed decision making. The Chief Privacy Officer has a nonvoting, advisory role on the Data Governance Council. Accordingly, the Chief Privacy Officer has insight into Council activities and initiatives and can identify privacy equities at an early stage to ensure incorporation of privacy compliance and risk mitigations.

Information Sharing and Safeguarding Governance Board

The DHS Information Sharing and Safeguarding Governance Board (ISSGB) serves as the steering committee and governance body for DHS collaboration on information sharing and safeguarding issues. The Chief Privacy Officer is a voting member of the ISSGB. During the reporting period, the Chief Privacy Officer:

- supported the designation of a DHS Chief Data Officer position as required by the *Foundations for Evidence-Based Policymaking Act of 2018* (Evidence Act);[6]
- advocated for effective oversight of Departmental use of publicly available information, including social media; and
- advocated for effective oversight of and policy development for the use of AI/ML.

Insider Threat Program

The Privacy Office participates in the operation of the Department's Insider Threat Program (ITP) in several ways. Department-wide and component-specific ITP activities are subject to the Department's privacy compliance documentation requirements. Privacy Office staff also participate in the Insider Threat Working Group (ITWG), which provides coordination, planning,

[6] Pub. L. No. 115-435, 132 Stat. 5529 (2018) (current version in scattered section of Title 5 and Title 44 of the U.S. Code).

and policy development for the Department. In addition, Privacy Office staff play a central role in the Insider Threat Oversight Group (ITOG).

The ITOG's primary purpose is to review all DHS policies and programs that govern and monitor for threats to DHS personnel, facilities, resources, and information systems. The group includes the Privacy Office, OGC's Intelligence Law Division, and CRCL. The ITOG meets quarterly to review the quarterly reports that provide anonymized details of all ITP activities and investigations and makes recommendations for new policies or procedures.

During the reporting period, Privacy Office staff worked closely with ITP leadership to start expanding the ITP to cover threats other than the inappropriate disclosure of classified information and to include non-cleared DHS personnel. Privacy Office staff are also working with other members of the ITOG to finalize auditing procedures.

Intelligence Product Reviews

Since 2009, the Privacy Office has reviewed I&A's draft intelligence products intended for dissemination outside the federal government, and materials used to brief threat information to the Department's non-federal partners. In addition, the Privacy Office reviews requests for information (RFI) related to source development, non-bulk information sharing, and foreign disclosure. In conducting these reviews, the Privacy Office analyzes the products against requirements of the Privacy Act, the FIPPs, and other relevant privacy laws and policies.

The Privacy Office's product review function is an ongoing, real-time operational service for the Department, requiring around-the-clock availability and quick response to I&A's requests for review of requests for information and intelligence products. During this reporting period, the Privacy Office reviewed 484 products containing finished intelligence (FINTEL), 135 briefing packages and 239 RFI (at all levels of classification). The Privacy Office also reviewed new or revised collection requirements drafted by I&A to ensure that DHS did not inadvertently solicit unauthorized or unneeded PII.

The Privacy Office, in cooperation with OGC's Intelligence Law Division and CRCL, is working to develop post-production audit procedures for the Department's raw intelligence reporting: Intelligence Information Reports (IIRs) and Open Source Intelligence Reports (OSIRs). The offices involved are continuing to develop an appropriate methodology for implementing periodic audits of all component-drafted IIRs and I&A-produced OSIRs.

International Information Sharing

The Privacy Office continues to provide subject matter expertise to the Department in its implementation of international information sharing agreements, including agreements with Mexico, the Migration Five countries, Visa Waiver Program countries, and countries executing Preventing and Combatting Serious Crimes Agreements.

2019 Evaluation of the 2011 U.S.-European Union Passenger Name Record Agreement
The Privacy Office was a member of the U.S. government delegation to evaluate the effectiveness of the 2011 U.S.-European Union (EU) Passenger Name Record (PNR) Agreement. The evaluation was designed to assess whether the Agreement is achieving its stated goals and benefiting transatlantic cooperation. A European delegation visited DHS facilities in September 2019 and the U.S. delegation visited the European Commission, Europol, and Passenger Information Units in Brussels and the Hague in October 2019. During the evaluation, the Privacy Office confirmed its oversight activities and queried the EU on privacy protections within its PNR programs. Additionally, DHS revisited its use and protection of PNR, demonstrating the Department's compliance with the 2011 Agreement.

Working Group Participation

The Privacy Office addresses several issues through active participation in a number of critical working groups. A description of some of the critical working groups and the Privacy Office's role in these bodies can be found in Appendix A.

IV. Compliance & Oversight

Privacy Compliance

The DHS privacy compliance documentation process includes four primary documents: PTAs, PIAs, SORNs, and, when applicable, Privacy Compliance Reviews (PCRs). Each of these documents have a distinct function in implementing privacy policy at DHS, and together they enhance the transparency and accountability of Department activities.

The Department's compliance document templates and guidance have served as best practice references for other federal agencies. See the Privacy Office website[7] for a detailed description of the compliance process, templates, and documents.

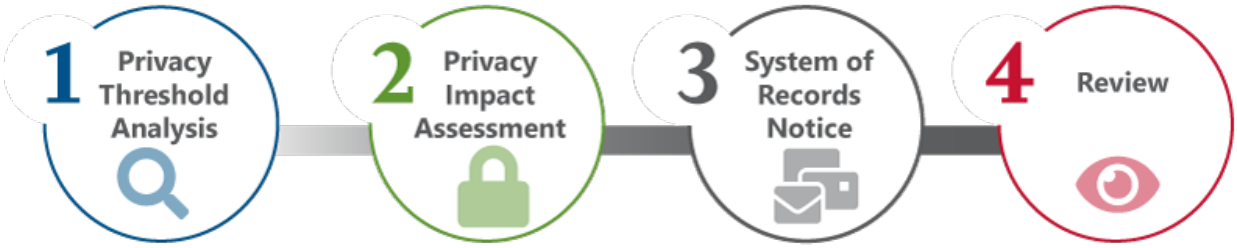


Figure 3: Privacy Compliance Process

The Privacy Office also conducts privacy reviews of the Office of Management and Budget (OMB) Exhibit 300 budget submissions and supports component privacy officers and privacy points of contact to ensure that component submissions meet privacy compliance requirements. The Privacy Office ensures the Department meets statutory requirements such as Federal Information Security Modernization Act of 2014 (FISMA)[8] privacy reporting.

- As of September 30, 2021, 99 percent of the Department's FISMA-reportable systems requiring a PIA had completed a PIA, and 100 percent of required SORNs were completed.
- Specific to the Department's COVID-19 response efforts, the Privacy Office reviewed and approved 241 PTAs, published and updated one pandemic response PIA, and published and updated one overarching public health-related SORN in the *Federal Register*.

[7] *See* https://www.dhs.gov/compliance
[8] 44 U.S.C. Chapter 35 (44 U.S.C. §§ 3551-3558).

Privacy Impact Assessments

The Chief Privacy Officer approved 150 new or updated PIAs during the reporting period. Lists of all new or updated PIAs can be found in the Privacy Office's Semi-Annual Section 803 Report. All unclassified PIAs are posted on the Privacy Office website.

Reporting Period	New Privacy Impact Assessments	Updated Privacy Impact Assessments
Fiscal Year 2021 (October 2020 – September 2021)	28	19
Fiscal Year 2020 (October 2019 – September 2020)	37	44
Fourth Quarter of Fiscal Year 2019 (July 2019 – September 2019)	12	10

System of Records Notices

The Chief Privacy Officer approved 34 SORNs during the reporting period. Lists of all new or updated SORNs can be found in Privacy Office's Semi-Annual Section 803 Report. All SORNs are posted on the Privacy Office website.

Reporting Period	System of Records Notices Published
Fiscal Year 2021 (October 2020 – September 2021)	10
Fiscal Year 2020 (October 2019 – September 2020)	22
Fourth Quarter of Fiscal Year 2019 (July 2019 – September 2019)	2

Computer Matching Agreements

The Chief Privacy Officer serves as the Chairperson of the DHS Data Integrity Board (DIB), which oversees and approves the use of the Department's Computer Matching Agreements (CMAs).[9] DIB members include the Inspector General, the CRCL Officer, the Chief Information Officer (CIO), and representatives of components that are currently sharing information pursuant to a CMA.[10]

[9] With certain exceptions, a matching program is "any computerized comparison of -- (i) two or more automated systems of records or a system of records with non-federal records for the purpose of (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under federal benefit programs. . . ." 5 U.S.C. § 552a(a)(8)(A)(i)(I).

[10] The Secretary of Homeland Security is required to appoint the Chairperson of the Data Integrity Board, which must include the Inspector General. 5 U.S.C. § 552a(u)(2). Other members of the DIB are designated by the Chairperson.

The Data Integrity Board conducted its annual CMA activity review and submitted the Department's Computer Matching Activity Annual Report [11] to OMB, covering Calendar Year 2019 in August 2020.

DHS continues to be party to 11 CMAs that can be found on the Privacy Office website. During the reporting period, nine of the agreements were extended for an additional year and two were renegotiated and will expire after eighteen months (unless extended).

Privacy Oversight

Privacy Compliance Reviews

The Privacy Office exercises its oversight function under 6 U.S.C. § 142 to ensure the Department's use of technology sustains, and does not erode, privacy protections,[12] primarily by conducting Privacy Compliance Reviews.[13]

The PCR framework emphasizes program involvement throughout the process to build trust with affected system or program managers. Privacy Compliance Reviews enable early issue identification and remediation, identification of lessons learned, privacy enhancing recommendations, updates to privacy compliance documentation, and a heightened awareness of privacy.

During the reporting period, the Privacy Office launched one new PCR. Privacy Office staff periodically assess the status of each PCR recommendation and list outstanding PCR recommendations on the Privacy Office's website.[14]

During the reporting period, the Privacy Office also reviewed a component-led PCR and provided additional recommendations. Component-led PCRs that are coordinated with the Privacy Office allow for a greater number of reviews to be completed each year and provide component privacy officers with additional opportunities to provide privacy oversight of component activities.

Privacy Investigations

The Homeland Security Act of 2002 gives the Chief Privacy Officer authority to conduct investigations of possible violations or abuse concerning the administration of the Department's programs or operations affecting privacy. During the current reporting period, the Privacy

[11] *See* https://www.dhs.gov/publication/computer-matching-agreement-activity-reports
[12] 6 U.S.C. § 142(a)(1).
[13] U.S. DEPARTMENT OF HOMELAND SECURITY, DHS INSTRUCTION 047-01-004, CHIEF PRIVACY OFFICER PRIVACY COMPLIANCE REVIEWS, *available at*: https://www.dhs.gov/publication/dhs-privacy-policy-instruction-047-01-004-privacy-compliance-reviews.
[14] *Available at*: https://www.dhs.gov/publication/outstanding-recommendations-privacy-compliance-reviews.

Office was informed of allegations that a component was collecting information on First Amendment-protected activities and engaging in retaliation against those individuals. As required,[15] the Privacy Office referred the allegations to the Office of Inspector General, which declined the matter. The Chief Privacy Officer instructed the Privacy Office to begin a privacy investigation into the allegations. As appropriate, the Privacy Office will publish results of the investigation.

Privacy Incidents

The Privacy Office manages privacy incident response for the Department, working to ensure that all privacy incidents are properly reported, investigated, mitigated, and remediated for each incident, in collaboration with the DHS Enterprise Security Operations Center (ESOC), component Security Operations Centers (SOCs), component privacy officers and PPOCs, and DHS management officials.

During the reporting period, the Privacy Office continued efforts to reduce privacy incidents and ensure proper incident handling procedures by:

- hosting monthly Department-wide Incident Practitioner meetings to identify and discuss trends and share incident response and mitigation best practices;
- analyzing incident trends and trouble-shooting incident causes to promote prevention efforts;
- meeting with components periodically to establish standards in the reporting and investigation of incidents;
- identifying vulnerabilities in data handling practices and reaching out to specific components for refresher trainings (i.e., at new employee orientations, town halls, participating in "Privacy Day"); and
- working with the Network Operations Security Center to develop a new enterprise incident database to make it easier for privacy staff to report and manage privacy incidents.

Incident Policies

The Privacy Office's DHS Privacy Incident Handling Guidance[16] (PIHG) serves as the foundation of DHS privacy incident response. DHS defines a privacy incident[17] as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an unauthorized purpose. The

[15] CHIEF PRIVACY OFFICER INVESTIGATIONS 047-01-002, *available at*: https://www.dhs.gov/publication/chief-privacy-officer-investigations-instruction-047-01-002.
[16] *See* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf
[17] DHS changed its long-standing definition of privacy incident to comport with OMB's definition of a **breach** in OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of PII* (Jan. 3, 2017), but added the final sentence to address suspected and confirmed incidents. The Privacy Office kept the term "privacy incident" to be consistent with other DHS incident types.

term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which result in a reasonable risk of harm.

Annual Privacy Incident Tabletop Exercise

During the reporting period, the Privacy Office planned and hosted the fourth Annual DHS Privacy Incident Tabletop Exercise in October 2021. The Privacy Office worked closely with FEMA's National Exercise Division, as well as the components' SOCs, led by the Enterprise SOC management team.

Incident Metrics

The Chief Privacy Officer, in consultation with the component privacy officers and other appropriate parties, evaluates reported privacy incidents and determines if the incident is a minor or major incident.[18] The Chief Privacy Officer is then responsible for ensuring that appropriate follow-up actions take place, including any required investigation and notification.

During this reporting period, 1,538 privacy incidents were reported to the DHS SOC. Figure 4 shows the total broken down by component.

Figure 4: Total number of privacy incidents by DHS component for the period July 1, 2019 – September 30, 2021

Component	Privacy Incidents July 1, 2019 – September 30, 2021
CBP	310
CISA	29
FEMA	97
FLETC	0
HQ	109
ICE	155
OIG	6
S&T	4
TSA	4
USCG	175
USCIS	638
USSS	11
Total	**1538**

[18] *See* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-006-privacy-incident-responsibilities-and-breach.

Major Incident Summaries

Update on Major Incident Involving FEMA's Federal Insurance and Mitigation Administration

DHS and FEMA's Federal Insurance and Mitigation Administration, Risk Management Directorate discovered that approximately 2.5 million individuals' information may have been impacted due to a vendor providing an inadequate level of user access controls to the information system containing data related to flood maps. The potential incident was identified while reviewing the execution of programmatic activities and reported to FEMA Privacy on February 12, 2020. This incident constitutes a major incident because the number of impacted individuals exceeds 100,000.

Members of the public shared limited PII to request changes to flood maps. The incident potentially impacted:

- members of the public who requested map changes;
- property owners directly impacted by the map changes;
- government officials involved in the map changes; and
- professionals involved in developing the data and submitting the map changes to FEMA.

To mitigate this incident FEMA retained the services of a third-party IT security vendor to perform an assessment of the implicated vendors' respective IT security environments and to assess the contents of FEMA data housed on vendor systems. The findings determined there was no evidence of intrusion and/or data spillage involving outside entities; no evidence of mishandling of PII data within the any of the vendors' environments; and no indication of any data breaches or compromise of the vendors' IT systems on which FEMA data is processed or stored. During the investigation, a separate configuration issue was identified that granted a small number of map change users' access to data they did not need. The misconfiguration was resolved.

During the investigation, compliance documentation, including PIAs, SORNs, and vendor contracts, were reviewed and modified appropriately to ensure compliance. In addition, the program has drafted and implemented new access control policies and procedures to ensure that vendors follow the proper protocols to prevent this type of event from happening in the future.

The Privacy Office sent an official close-out memorandum of this incident to Congress on July 26, 2021.

Major Incident Involving Potentially Malicious Network Activity

In December 2020, the Department became aware of potentially malicious network activity and began responding to a significant cybersecurity incident. The Privacy Office immediately established a dedicated response team to focus exclusively on this incident. An investigation into the facts surrounding the activities resulted in the declaration of a major incident.

The dedicated response team collaborated with the CISA. The collaborating team investigated the incident to determine potential impacts. DHS conducted remediation actions to promote prevention efforts related to information systems.

Special Protected Classes – Unauthorized Disclosures

As discussed previously, the Privacy Office and CRCL continue to share responsibilities for ensuring the proper handling of Section 1367 information. The Privacy Office and CRCL have implemented a notification process whereby the two offices share incidents of unauthorized Section 1367 disclosures with each other. The two offices then work together to ensure all incidents are appropriately investigated, addressed, and resolved. Of the 1,538 total reported privacy incidents during this reporting period, there were 55 incidents related to the unauthorized disclosure of Special Protected Classes information. Of these 55 reported incidents, 52 were confirmed incidents; one was investigated and found not to be related to a Special Protected Class; and two were investigated and it was determined there was no breach.

Privacy Complaints

The Privacy Office is responsible for ensuring that the Department has procedures in place to receive, investigate, respond to, and, when appropriate, provide redress for privacy complaints. Details regarding the number and nature of complaints of alleged violations received by the Department, and a summary of the disposition of such complaints, when available, are included in the Privacy Office Semi-Annual Section 803 Report.

Privacy Act Amendment Requests

The *Privacy Act* permits an individual, defined by the *Privacy Act* as a U.S. citizen or Legal Permanent Resident (LPR), or defined as a covered person by the *Judicial Redress Act of 2015*, to request amendment of his or her own records.[19] As required by DHS Privacy Policy Guidance Memorandum 2011-01, Privacy Act Amendment Requests[20] (Privacy Policy Directive 140-08), Component Privacy Officers and FOIA Officers are responsible for tracking all Privacy Act Amendment requests and reporting the disposition of those requests to the Privacy Office. The Privacy Office serves as the repository for those statistics.

[19] 5 U.S.C. § 552a(d)(2). By policy, DHS extends Privacy Act protections to all individuals whose information is maintained in a system that contains both U.S. person information and non-U.S. person information.
[20] *See* https://www.dhs.gov/xlibrary/assets/privacy/privacy-policy-guidance-memorandum-2011-01.pdf

Figure 6: Privacy Act Amendment Requests received by DHS during the reporting period by component and disposition.

Privacy Act Amendment Requests July 1, 2019 – September 30, 2021						
Component	**Received**	**Granted**	**Denied**	**Administrative Closure[21]**	**Pending**	**Referred**
USCG	1	0	0	0	0	1
CBP	43	8	20	10	1	4
ICE	29	2	11	3	0	13
FPS	1	1	0	0	0	0
TOTALS	**48**	**3**	**26**	**4**	**5**	**10**

Non-Privacy Act Redress Programs

DHS also provides redress for individuals impacted by DHS programs through several other mechanisms that have a privacy nexus, including:

OBIM Redress Program. OBIM maintains biometric information that is collected in support of DHS missions. One of the main goals of the redress program is to maintain and protect the integrity, accuracy, privacy, and security of information in its systems.

- OBIM reviewed and responded to four redress requests from OBIM FOIA, and four DHS TRIP redress requests.

Transportation Sector Threat Assessment and Credentialing Redress. TSA's I&A Security Threat Assessment Division (STAD) conducts security threat assessments and completes adjudication services in support of TSA's mission to protect U.S. transportation systems from individuals who may pose a threat to transportation security. I&A STAD provides daily checks on over 15 million transportation sector workers against the U.S. Government's Terrorist Screening Database. I&A STAD provides a redress process that includes both appeals and waivers for transportation sector workers who believe they were wrongly identified as individuals who pose a threat to transportation security. Typical redress requests have involved documentation missing from initial submissions, immigration issues, or requests for appeals and waivers for criminal histories. During the reporting period, I&A STAD granted 4,880 appeals and denied 597. Additionally, I&A STAD granted 2,049 waivers and denied 351.

[21] DHS may administratively close requests that are not reasonably described. Requesters who do not respond to a request for additional information within thirty (30) working days, may also have their request administratively closed at DHS's discretion. This administrative closure does not prejudice the requester's ability to submit a new request for further consideration with additional information.

V. Engagement, Education, and Reporting

The Privacy Office engages with internal and external stakeholders and the public. These engagements promote transparency and bring a diversity of views into the Department's decision-making processes. The Privacy Office also provides privacy training and conducts privacy awareness activities and is responsible for congressionally required reporting.

Engagement

Conferences and Events

The Chief Privacy Officer and Privacy Office staff regularly present at conferences and participate in public meetings to educate and inform both the public and private sectors on DHS privacy policies and best practices. During the reporting period, the Chief Privacy Officer highlighted DHS's approach to privacy as a speaker at several events. A representative sample include:

- International Association of Privacy Professionals (IAPP) Global Privacy Summit, panel participant. April 12 – 13, 2021.
- Silicon Valley Innovation Program Demo Week, panelist. September 16, 2021.
- Federal Privacy Council Summit, panel organizer and participant. November 3, 2021.
- PrivSec Global, keynote address, December 1, 2021.
- IC Privacy and Civil Liberties Summit, panel organizer and participant with the then-Senior Official Performing the Duties of the Under Secretary for Information and Analysis Cohen and the Under Secretary for Policy January 19, 2022.

Data Privacy and Integrity Advisory Committee

The Data Privacy and Integrity Advisory Committee (DPIAC) provides advice to the Department at the request of the Secretary and Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to PII, as well as data integrity, transparency, and other privacy-related matters.[22] DPIAC members have broad expertise in privacy, cyber, security, and emerging technology, and they come from large and small companies, academia, state and local governments, and the non-profit sector. Members hold public meetings to receive updates from the Privacy Office on important privacy issues and to provide recommendations based on taskings from the Chief Privacy Officer.

[22] The Committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. § 451 and operates in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. App 2. DPIAC members serve as Special Government Employees and represent a balance of interests on privacy matters from academia, the private sector (including for-profit and not-for-profit organizations), state government, and the privacy advocacy community.

The DPIAC conducted one public meeting during the reporting period during which the Committee received an update on Privacy Office activities and the Policy and Emerging Technologies Subcommittees provided an update on their outstanding taskings. In addition, the Privacy Office solicited for new members to replace vacancies on the Committee. In November 2021, Secretary Mayorkas appointed 17 new or returning members.

All DPIAC reports, along with membership and meeting information, are posted on the Privacy Office website[23].

Privacy and Civil Liberties Oversight Board (PCLOB)

The Privacy Office participates in public and private meetings with the PCLOB, which was established as an independent oversight board within the Executive Branch by the *Implementing Recommendations of the 9/11 Commission Act*.[24] During the reporting period, the PCLOB, in both their advisory and oversight capacities, was actively engaged with DHS. In addition, the Board continues to act in a consultative role on the annual Privacy and Civil Liberties Assessment Reports required by Executive Orders 13636 and 13691.

Privacy Advocates

Regular engagement with privacy advocates promotes understanding of various viewpoints and builds trust. During the reporting period, the Privacy Office offered several opportunities for privacy advocates to meet with Department leadership, including a wide-ranging discussion with Secretary Mayorkas regarding the Department's operations. The Privacy Office also arranged a meeting between privacy advocates and the then-Senior Official Performing the Duties of the Under Secretary for Intelligence and Analysis to discuss protecting privacy while addressing the threats associated with domestic violent extremism and coordinated a meeting with USCIS to discuss privacy concerns related to the use of automated tools in vetting processes.

The DHS Privacy Office, in partnership with both TSA and CBP, also engages with privacy and civil liberties groups regularly in advance of the launch of new biometric technologies, in order to update the groups on the pilots and the planned privacy protections, as well as answer questions. During this reporting period, TSA hosted advocacy groups at virtual roundtables in August 2020, January 2021, and June 2021. Attendees included the PCLOB, the American Civil Liberties Union, the Electronic Frontier Foundation, the Electronic Privacy Information Center, the Center for Democracy and Technology, and the Cato Institute.

International Engagement & Outreach

DHS works closely with international partners, including foreign governments and major multilateral organizations, to meet its national security mission on a global stage. When those

[23] *See* www.dhs.gov/privacy-advisory-committee
[24] Pub. L. No. 110-53, Title VIII, § 801, 121 Stat. 266, 358 (2007).

engagements involve the sharing of PII, the Privacy Office ensures that those engagements include privacy protections, and privacy compliance documentation provides transparency about how the Department handles that PII.

The Privacy Office supports Department and U.S. government international priorities by providing input to interagency and Department engagements. The Privacy Office contributes to DHS positions in the Migration Five, a forum made up of the United States, Canada, New Zealand, Australia, and the United Kingdom for cooperation on migration and security. The Privacy Office also supports departmental participation in privacy issues addressed by the Organization for Economic Cooperation and Development by providing input on the work of the Committee on Digital Economy Policy and the Data Governance and Privacy Working Party.

In addition, the Privacy Office participates in the Department's International Pre-Deployment Training, a week-long training course for new DHS attachés deployed to U.S. embassies worldwide. The Privacy Office provides an international privacy policy module to raise awareness of the potential impact of misperceptions regarding DHS privacy policy, practice, and global privacy policies on DHS's international work.

Education: Privacy Training and Awareness

The Privacy Office develops and delivers a variety of ongoing and one-time privacy trainings to DHS personnel and key stakeholders. Staff training and awareness are key to preventing accidental privacy incidents. All DHS personnel are required to understand, identify, and mitigate privacy risks, and proactively safeguard PII. Privacy Office and component privacy training and awareness activities are also detailed in the *Privacy Office Semi-Annual Reports to Congress,* available on the Privacy Office website.

Reporting

Privacy Reports

- Annual Privacy Office Report[25]: summarizes the activities and accomplishments of the Privacy Office.
    - Semi-annual Section 803 Report[26]: summarizes key privacy compliance artifacts, privacy policies, privacy complaints, and privacy training and awareness activities.
- Computer Matching Agreement Report[27]: annual review of DHS computer matching activity.

[25] *See* https://www.dhs.gov/publication/privacy-office-annual-reports
[26] *See* https://www.dhs.gov/publication/dhs-section-803-reports-congress
[27] *See* https://www.dhs.gov/publication/computer-matching-agreement-activity-report

- Data Mining Report[28]: annual summary of DHS programs that conduct pattern-based queries, searches, or analyses of one or more electronic databases to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activities.
- Privacy and Civil Liberties Assessment Report[29]: Senior Agency Officials for privacy and civil liberties assess the privacy and civil liberties impacts of the activities their respective departments and agencies have undertaken to implement two Executive Orders on cybersecurity and publish their assessments annually in a report compiled by the Privacy Office and CRCL.
- Social Security Number Fraud Prevention Act Report[30]: summarizes DHS actions to reduce the collection and use of SSNs. (Sunset in 2021.)

FOIA Reports

- Annual FOIA Report[31]: includes Component-specific and Department-wide data on FOIA processing, including the number of FOIA requests received and processed, average response times, and backlogs.
- Chief FOIA Officer Report[32]: documents actions taken by the Department to advance transparency and to ensure DHS effectively administers FOIA.

[28] *See* https://www.dhs.gov/publication/dhs-data-mining-reports
[29] *See* https://www.dhs.gov/publication/executive-orders-13636-and-13691-privacy-and-civil-liberties-assessment-reports
[30] *See* https://www.dhs.gov/publication/social-security-number-fraud-prevention-act-report
[31] *See* https://www.dhs.gov/foia-annual-reports
[32] *See* https://www.dhs.gov/dhs-chief-foia-officer-reports

VI. Business Operations

During the reporting period, the Business Operations team conducted the following:

- Leveraged interagency agreements to collect $4,061,155 in reimbursable funds which enabled components to utilize the Privacy Office's FOIA and privacy support services contract vehicles. This efficiency provided surge staffing support to manage component FOIA backlogs and fund infrastructure and license costs related to FOIAXpress, the web-based application that processes FOIA and Privacy Act requests.
- Updated the internal and external communications plans.
- Updated the Awards Policy.
- Trained staff on records management responsibilities.
- Created career ladders for both the FOIA and Privacy divisions.
- Enhanced staff communications through monthly town hall meetings and other events.
- Established and maintained a Twitter account for the Chief Privacy Officer.
- Reinstituted the Staff Advisory Council to address staff morale and improve management services.
- Reinstituted the Privacy Office Reconstitution Team to address the needs and concerns of Privacy Office staff and to ensure maximum communication to all staff during the pandemic.

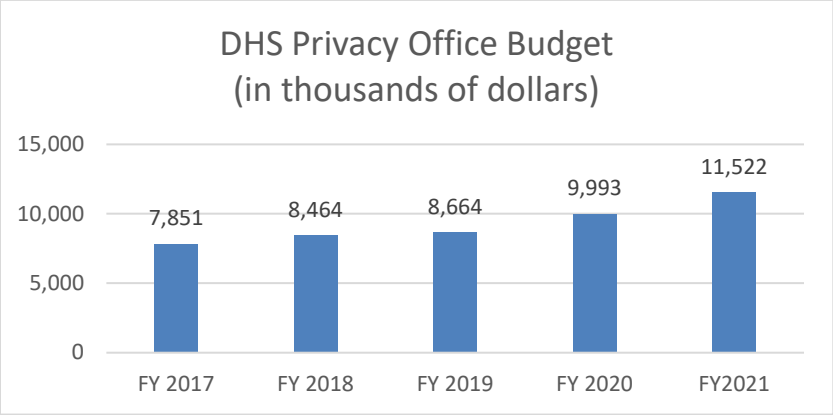
Additionally, the Privacy Office conducted outreach, sponsored leadership development opportunities, provided skills training, and tapped into new sources to recruit diverse talent to support its mission and advance goals.

Workforce

During the reporting period, the Privacy Office hired 13 federal positions, for a total of 52 federal employees, one detailee, and 13 contractors, including the following back-filled positions:

- Chief Privacy Officer
- Deputy Chief FOIA Officer
- Two Attorney Advisors
- Senior Advisor to the Deputy Chief FOIA Officer
- Director, Privacy Policy
- Program and Management Analyst (Communications)
- Program and Management Analyst (Business Operations)
- Government Information Specialist (Policy)
- Government Information Specialist (Oversight)
- Four Government Information Specialists (FOIA)

Budget



In Fiscal Year 2021, the Privacy Office's budget was $11,522,000 and was allocated as follows:

The Privacy Office maximized its resources by:

- enhancing operational and financial performance by allowing components to purchase over $2,0470,237 in FOIA and privacy support services using current contract vehicles to support the Department's privacy and disclosure requirements. This reduced acquisition administrative costs and created time and resource efficiencies; and
- leveraging intra-agency agreements with Departmental offices and components to reimburse the Privacy Office $542,987 for infrastructure and license costs related to FOIAXpress, the web-based application used for processing FOIA and Privacy Act requests.

Staff Training and Development

To build a workforce in which employees can contribute at their highest level, the Privacy Office encouraged its staff, as well as privacy and FOIA professionals throughout the Department, to seek development opportunities to improve efficiency and productivity. The Privacy Office conducted numerous privacy and FOIA trainings and seminars to emphasize its commitment to developing and maintaining an effective, mission-focused, diverse, and knowledgeable workforce.

Privacy Office staff attended the following training and development opportunities:

- IAPP Global Privacy Summit;
- Federal Privacy Summit;
- Federal Privacy Bootcamp;
- American Society of Access Professionals Virtual National Training Conference; and
- IAPP U.S. Private Sector Privacy Training Online.

Appendix A – Working Groups

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: -PTA submissions for each dataset targeted for onboarding, as well as updates to the DSB PIA and SORN for each dataset onboarded for any new use or user of a dataset. -Approval of all datasets ingested, and 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 FIPPs 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 (IDII DGWG). 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 PII. Specifically, the P&O team developed and edited the IDII 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.
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 mitigation activities develop, the Privacy Office will continue to focus on the safeguards around the use of Sensitive PII, the impact to the individual, and compliance with privacy laws and policies.
Privacy, Civil Rights, and Civil	The PCRCL Working Group is comprised of senior privacy and civil liberties officials from several	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

Liberties (PCRCL) Working Group	departments and agencies supporting the implementation of NSPM-9, *Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise.*	(NVC) Governance Board. Privacy Office staff are also members of the Working Group, which 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 Department's *2019 Strategic Framework for Countering Terrorism and Targeted Violence* and national strategies.	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.