Department of Homeland Security

Privacy Office Fiscal Year 2022 Annual Report to Congress

December 2023

Homeland Security

Message from the Chief Privacy Officer

It is my honor to serve as the Department of Homeland Security (DHS) Chief Privacy Officer and Chief Freedom of Information Act (FOIA) Officer. I am pleased to deliver this Annual Report on the Privacy Office's activities to embed privacy safeguards and enhance transparency in all DHS activities.

This report charts the Privacy Office's advances during former Chief Privacy Officer Lynn Parker Dupree's tenure. During this reporting period, the Privacy Office engaged with internal and external stakeholders to enact a forward-looking agenda that protects privacy and enhances transparency. One hallmark of this work is the development of strategic partnerships that position the Privacy Office as a critical partner in the identification, development, and use of privacy enhancing technologies to accomplish the Department's mission. The use of these technologies is a force multiplier for the Privacy Office's continual efforts to build privacy by design into Department operations, as it continues its work evaluating programs and systems for privacy risks and appropriate mitigation measures while engaging in the Department's policy-making processes. Additionally, the Privacy Office has invested in technologies to improve privacy compliance and ensure maximum transparency into the Department's use, collection, and destruction of personally identifiable information.

As the Department's use of systems and technology evolves, so too must the Privacy Office. Accordingly, this report also discusses the Privacy Office's engagement across the Department and with stakeholders on cross-cutting and emerging issues, like the use of Artificial Intelligence and biometrics.

The Department is committed to enhancing openness and transparency and ensuring the protection of privacy, civil rights, civil liberties, and human rights of the communities we serve. The Privacy Office looks forward to providing future updates on its ongoing work to deliver on this promise.

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

Sincerely,

Mason C. Clutter
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 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 O. 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 R. Turner
Chairman, House Permanent Select Committee on Intelligence

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

DHS Privacy Office
Fiscal Year 2022 Annual Report to Congress
Table of Contents

Contents

Executive Summary

This report highlights the DHS Privacy Office's notable strategic and programmatic activities during Fiscal Year (FY) 2022, enabling the Department to accomplish its mission while embedding and enforcing privacy safeguards and transparency in all DHS activities.

The rapid development in technology and growth in Department operations requires that the Privacy Office remain nimble and adaptable to achieve its mission. As highlighted in this report, the Privacy Office proactively identified privacy enhancing research and development as a strategy to integrate privacy protections into the Department's technical architecture and streamline programmatic operations. These efforts include collaborative work across the Department to identify, develop, and implement privacy enhancing technologies in the near and long term, and the integration of technology into the privacy compliance process to streamline operations and enable modern business practices that improve efficiency and efficacy. Together, these efforts act as a force multiplier for the Department's information governance framework for identifying and mitigating privacy risks.

The Privacy Office also continued its work to reinvigorate efforts to deepen and expand engagement with a diverse set of external stakeholders. During FY 2022, the Privacy Office built on the successful engagement with privacy advocates and Secretary Mayorkas in November 2021 to host program and operational-specific engagements and to participate in public-facing events both in DC and outside of the National Capitol Region. These activities improved understanding of Department programs and ensured a broad set of interests and experiences informed the Department's decision-making processes.

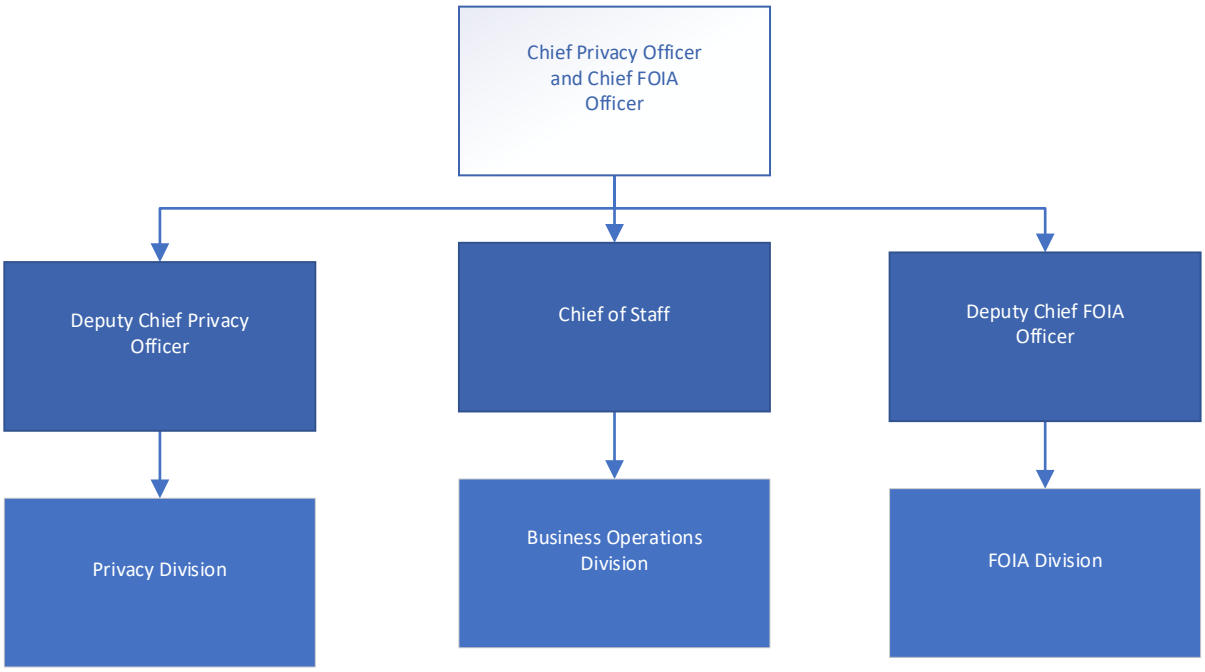
Additionally, the Privacy Office also worked to address and bring critical attention to cross-cutting and emerging issues through the compliance documentation process and continuous engagement in the Department's policymaking process. The Privacy Office's work on these issues, including the use of biometrics, the deployment of artificial intelligence and machine learning, and the use of body worn cameras, ensured privacy risks were appropriately identified and mitigated early in the process.

Finally, this report highlights the Privacy Office's programmatic and organizational advancement on its mission. These achievements include: successfully handling increased compliance documentation with 30 new or updated Privacy Impact Assessments completed and 13 System of Records Notices published; extending or renegotiating eight Computer Matching Agreements; responding to 921 reported privacy incidents; filling 7 additional federal positions; facilitating Components' purchase of nearly $7 million in Freedom of Information Act and privacy support services using current contract vehicles; and closing a 2001 Office of Inspector General recommendation.

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 division is critical to ensuring privacy and transparency are integrated into the Department's mission.

Figure 1: DHS Privacy Office Organizational Chart



The Privacy Division collaborates with Privacy Officers appointed by Components,[1] as well as privacy points of contact[2] and program offices on the development of privacy policy and preparation and adjudication of privacy compliance documentation.

Table 1: DHS Privacy Divisions, Component Privacy Officers, and Privacy Points of Contact

DHS Privacy Division	Component Privacy Officers	Privacy Points of Contact
• Privacy Policy and Oversight Team • Privacy Compliance Team	• Cybersecurity and Infrastructure Security Agency (CISA)	• Countering Weapons of Mass Destruction Office (CWMD)

[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] 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 program managers and the Privacy Office to manage privacy matters within DHS.

DHS Privacy Division	Component Privacy Officers	Privacy Points of Contact
	• 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 (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) • Federal Protective Services (FPS)	• Office of the Chief Human Capital Officer (OCHCO) • Office of the Citizenship and Immigration Services Ombudsman (CISOMB) • Office of Operations Coordination (OPS) • Office of Public Affairs (OPA) • Office of the Chief Security Officer (CSO) • Office of Immigration Statistics (OIS)

The Privacy Policy and Oversight Team is led by a Senior Director and comprises teams that are responsible for 1) privacy investigations and incident responses; 2) privacy policy development; 3) oversight of finished intelligence disseminated outside the Department; 4) information sharing; 5) computer matching agreements; and 6) other duties assigned by the Chief Privacy Officer.

The Privacy Compliance Team is also led by a Senior Director. Team members are assigned one or more Components with which the team member maintains close contact to assess and help fulfill the Component's privacy compliance requirements. The compliance process is discussed below.

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. Privacy-enhancing technologies promise the ability to control the sharing and use of sensitive information while minimizing the risk of unauthorized use. These technologies have been under development by researchers for nearly four decades but have been slow to migrate from the research lab into operational use.

The Privacy Office is developing a multi-pronged approach to be a proactive partner in identifying and encouraging the development and use of these emerging technologies. This approach includes strategic investments in the refinement of privacy enhancing technologies that are in use successfully in other contexts; encouraging the development of privacy enhancing technologies that can be deployed in the next few years; and spreading awareness and interest in promising methodologies in the academic field.

Image 1: Former Chief Privacy Officer and Chief FOIA Officer Lynn Parker Dupree opens the *Privacy Enhancing Technologies for the Homeland Security Enterprise Workshop* with a keynote address.

A. Workshop on Privacy Enhancing Technologies for the Homeland Security Enterprise

On June 21, 2022, the Privacy Office and the Science and Technology Directorate's Center for Accelerating Operational Efficiency, a DHS Center of Excellence, co-hosted a workshop designed to identify solutions for operational challenges within the Homeland Security Enterprise using privacy enhancing technologies.

Through a series of presentations and discussions, the workshop facilitated an exchange of information between researchers and practitioners to expand awareness and understanding of promising methodologies and potential uses for privacy enhancing technologies in the Homeland Security enterprise.

Participants in the workshop included researchers in academia and the private sector, Department program officials, and the National Science Foundation. The program also brought awareness to existing programs and resources designed to transition research into practice.

The workshop featured:

- Potential uses of privacy enhancing technologies.
- Researchers working on a range of privacy enhancing technologies, including secure multiparty computation, private set intersection, secure anonymous recording linking, differential privacy, and other methods for privacy preserving data sharing and analysis.

Image 2: Former Chief Privacy Officer and Chief FOIA Officer Lynn Parker Dupree participates in a panel discussion during the *Privacy Enhancing Technologies for the Homeland Security Enterprise Workshop.*

- Discussions about potentially transitioning research to pilot programs and operational capacities within the Homeland Security Enterprise.

The Privacy Office continues to work with the Center for Accelerating Operational Efficiency to build off the momentum generated by the workshop. This includes the creation of an academic lecture series highlighting research on privacy enhancing technologies.

B. Technical Exchange Meeting on Digital Identities

On April 26, 2022, the Privacy Office convened a Technical Exchange Meeting to provide feedback on work at U.S. Citizenship and Immigration Services to develop digital immigration credentials (such as U.S. Permanent Resident Cards). U.S. Citizenship and Immigration Services has partnered with the Science and Technology Directorate Silicon Valley Innovation Program on this work. The Silicon Valley Innovation Program funds innovation and works with private sector partners to advance Homeland Security solutions.

The Privacy Office identified and invited privacy advocates with technical expertise and experience to participate in the meeting. As explained during the meeting, one of the goals of the project is to prioritize privacy and security to ensure individual control over and consent to use data. Accordingly, Silicon Valley Innovation Program and U.S. Citizenship and Immigration Services are researching the use of verifiable credentials that meet the standards issued by the World Wide Web Consortium (W3C).

The Silicon Valley Innovation Program and U.S. Citizenship and Immigration Services will coordinate with the Privacy Office to seek feedback from privacy advocates as the work progresses.

C. Privacy Compliance Documentation Platform (PRIVCATS 2.0)

In June 2022, the Privacy Office initiated a project to build out its internal privacy compliance document tracking system known as PRIVCATS. First, the Privacy Office identified Component mission-critical needs for a privacy compliance tracking system and learned how PRIVCATS could be incorporated into Component internal review processes. The Privacy Office then worked with the DHS Office of the Chief Information Officer to modify PRIVCATS and provide Component privacy professionals access to the system. The expanded system, PRIVCATS 2.0, is anticipated to enable the tracking of critical deadlines and additional required privacy compliance documentation, provide automated notification of expiring compliance documentation, and allow for robust monitoring of program compliance metrics.

Updates regarding the rollout of PRIVCATS 2.0 and the continued development of the system will be included in future reports.

D. Section Conclusion

During the reporting period, the Privacy Office partnered with offices in the Science and Technology Directorate, which have experience and expertise in technology research and development, to capitalize on the potential to integrate privacy enhancing technologies into the Department's operations. The signature accomplishment was the inaugural *Workshop on Privacy Enhancing Technologies for the Homeland Security Enterprise*. The Privacy Office and Science and Technology Directorate also collaborated to facilitate expert conversations among a variety of stakeholders with diverse viewpoints and experiences, including privacy advocates, technologists, start-ups, and academic researchers.

The Privacy Office also made significant progress in adapting business processes and technological innovations that have proven useful in the private sector into the Department's privacy compliance processes. The development of PRIVCATS 2.0 provided a department-wide advanced collaborative platform that supports the timely creation and processing of privacy compliance documents, reduces administrative burden, and supports the identification of privacy compliance best practices.

II. Engagement and Awareness Building

Regular engagement with stakeholders promotes understanding of various viewpoints and builds trust with the communities we serve. The Privacy Office tailors its outreach and community engagement efforts to introduce a diverse set of views and experiences into the Department's decision-making processes. To accomplish this, the Privacy Office implemented a multi-pronged strategy that involved proactive community and public engagement and engagements with advisory and oversight bodies.

A. Community Engagement

In November 2021, the Privacy Office hosted a meeting between Secretary Mayorkas and privacy advocates in which Secretary Mayorkas participated in a wide-ranging discussion regarding the Department's operations.

The Privacy Office also plays a critical role in connecting Components and programs with privacy advocates and other stakeholders. The Privacy Office maintains connections with privacy experts that have a diversity of views, experiences, and expertise, and works with Components and programs to organize engagement opportunities that are tailored to ensure constructive feedback.

Image 3: Chief Privacy Officer Dupree and CISA Director Jen Easterly at the CISA Open House.

On September 16, 2022, the Privacy Office invited privacy advocates to participate in an Open House hosted by the Cybersecurity and Infrastructure Security Agency (CISA). During the Open House, CISA leadership briefed participants on high-profile and potentially privacy-sensitive programs.

On September 22, 2022, the Privacy Office also hosted a meeting for privacy advocates with the DHS Face Recognition Working Group. During the meeting, DHS heard from experts on key aspects of a potential governance structure for the Department's use of face recognition technologies. The feedback received during this engagement will inform the DHS Face Recognition Working Group efforts moving forward.

B. Public Outreach

The Chief Privacy Officer regularly participates in activities to educate and inform the public and private sectors on DHS privacy policies and best practices. These opportunities include participation in conferences, public meetings, and media interviews. During the reporting period, the Chief Privacy Officer highlighted DHS's privacy mission as a speaker at several events. A representative sample includes:

- Federal Privacy Council Summit, panel organizer and participant, November 2021.
- PrivSec Global, keynote address, December 2021.
- U.S. Intelligence Community Privacy and Civil Liberties Summit, panel organizer and participant, January 2022.
- *Federal News Radio*, interview, February 2022.
- Homeland Security & Defense Foundation, April 2022.
- Joint Evidence Council, presenter and moderator, May 2022.
- *USA Today*, interview, July 2022.
- Silicon Valley Innovation Program Outreach, speaker, September 2022.

C. 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 involve personally identifiable information, as well as data integrity, transparency, and other privacy-related matters.[3] DPIAC members have broad expertise in privacy, cyber, security, and emerging technology, across large and small companies, academia, state and local governments, and the non-profit sector. Members hold public meetings and receive updates from the Privacy Office on important privacy issues and provide recommendations based on taskings from the Secretary or Chief Privacy Officer.

The DPIAC conducted two public meetings during the reporting period. On February 22, 2022, the Committee met to receive updates from the standing subcommittees: Policy and Emerging Technologies. At this meeting, the Chief Privacy Officer also issued a new tasking requesting input on a potential governance structure for the Department's use of commercial data. On April 26, 2022, DPIAC presented draft reports responding to the Chief Privacy Officer's previous taskings related to information sharing and migration to the cloud.

The Privacy Office posts all DPIAC reports and membership and meeting information on the Privacy Office website.[4]

D. Engagement with the Privacy and Civil Liberties Oversight Board (PCLOB)

During the reporting period, DHS participated in engagements related to PCLOB's advisory and oversight capacities. The PCLOB is an independent agency within the Executive Branch, established by the *Implementing Recommendations of the 9/11 Commission Act*.[5] A list of all

[3] The Committee was established by the Secretary of Homeland Security under 6 U.S.C. § 451 and operates in accordance with the provisions of the Federal Advisory Committee Act, 5 U.S.C. ch. 10. DPIAC members serve as Special Government Employees.
[4] *See* www.dhs.gov/privacy-advisory-committee.
[5] Pub. L. No. 110-53, Title VIII, § 801, 121 Stat. 266, 358 (2007).

PCLOB projects involving DHS is available on the Privacy and Civil Liberties Oversight Board website.

E. Section Conclusion

In FY 2022, the Privacy Office reinvigorated its community engagement and public outreach efforts. Specifically, the Privacy Office built on the successful engagement between privacy advocates and Secretary Mayorkas in November 2021 to host additional tailored engagements with privacy experts, including a CISA Open House and a briefing with the Face Recognition Working Group. The Privacy Office also expanded its public outreach efforts, participating in major conferences in and outside of the DC area. Additionally, the Privacy Office continued to play a key role as a liaison with external privacy advisory and oversight bodies.

III. Cross-Cutting and Emerging Issues

Privacy is ever evolving, and protecting privacy is critical to meet the Department's mission as programs and technology change. During the reporting period, the Privacy Office was involved in the DHS policy-making process, and through its work on privacy compliance documentation, involved in key issues that implicate privacy, including the use of Artificial Intelligence, biometric information, and body worn cameras.

A. Artificial Intelligence

The Privacy Office is operationalizing privacy risk assessment and mitigation at the U.S. Department of Homeland Security for artificial intelligence and machine learning technology by:

- assessing potential privacy risks of and mitigation measures for artificial intelligence and machine learning technology identified through the privacy compliance process, including Privacy Threshold Analysis documents, Privacy Impact Assessments, and System of Records Notices;
- participating in Departmental and external working groups; and
- ensuring that artificial intelligence and machine learning activities adhere to existing privacy governance frameworks.

B. Biometric Information Sharing and Identity Verification

The Privacy Office ensures Fair Information Practice Principles are applied to the Department's collection, maintenance, and use of personally identifiable information, including biometric data. This is accomplished by implementing Privacy Office recommendations in Privacy Compliance Reviews and embedding safeguards in Privacy Impact Assessments, as well as including privacy requirements in information sharing agreements to ensure data quality and integrity, while supporting the Department's mission.

During the reporting period, the Privacy Office provided privacy guidance in the negotiation and implementation of biometric interoperability and information sharing agreements with other agencies and addressed privacy issues related to international biometric information sharing.

Biometric-based information sharing 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. Throughout the reporting period, Privacy Office team members joined Departmental biometrics working groups. The Privacy Office also continues to work with Components and program offices on the development of Departmental policies surrounding these efforts.

C. Use of Body Worn Cameras in Law Enforcement

Following the issuance of President Biden's May 25, 2022, Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety, the Privacy Office began supporting the Department's efforts to fulfill each of the executive order's requirements, including the use of body worn cameras. Privacy Office team members participated in discussions and policy development on this and other policing-related topics.

The Privacy Office also worked to ensure Components that will use body worn cameras have the capacity to process Freedom of Information Act requests for body worn camera footage.

D. Section Conclusion

Changes in law, policy, and technology presented the Department with opportunities to use artificial intelligence, biometric information, and body worn cameras. The Privacy Office's active engagement in interagency working groups and robust compliance processes ensured that the Department appropriately addressed and mitigated potential privacy risks related to the use of these and other emerging technologies.

IV. Privacy Policy

The Privacy Office is deeply engaged in the Department's policy-making processes. Below are notable updates to privacy policies and other policy-related accomplishments from the reporting period.

A. Acquisition Regulations and Departmental Policies

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

B. Fusion Centers

The Privacy Office established and continues to enhance a robust privacy protection framework within the U.S. Department of Homeland Security Fusion Center program, both at the national and state levels. The Privacy Office reviews fusion center privacy policies to ensure they meet the Information Sharing Environment Privacy Guidelines, assists fusion centers with incorporating privacy protections in new policies, and shares privacy compliance document templates. The Privacy Office also collaborates with the Office for Civil Rights and Civil Liberties, Intelligence & Analysis, and the Office of Partnership and Engagement to train fusion center privacy officers and analytical staff.

C. Special Protected Classes Information

The Privacy Office and Office for Civil Rights and Civil Liberties share responsibilities under confidentiality provisions of Title 8, United States Code, Section 1367,[6] (herein Section 1367) related to incidents of unauthorized disclosures of information of certain non-citizen victims of crimes, including applicants and recipients of immigration relief under the Violence Against Women Act and the Victims of Trafficking and Violence Prevention Act of 2000. The release of personally identifiable information about individuals in these protected classes could subject them to further harm and reprisal.

During the reporting period, the Privacy Office hosted three quarterly meetings with the Office for Civil Rights and Civil Liberties and Components that work with individuals and information about individuals in Special Protected Classes: U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), Office of Biometric Identity Management (OBIM), and U.S. Citizenship and Immigration Services (USCIS).

Additionally, the Privacy Office hosted a Special Protected Classes Unauthorized Disclosure Forum to refresh and educate U.S. Department of Homeland Security privacy points of contact and privacy incident practitioners on requirements for safeguarding this information.

[6] 8 U.S.C. § 1367, "Penalties for Disclosure for Information."

D. Information Sharing and Intelligence Activities

The Privacy Office provides specialized expertise on Information Sharing and Access Agreements and programs to support the Department's information sharing activities with other federal agencies, the Intelligence Community, state and local entities, and international partners.

The Privacy Office evaluates information sharing requests that involve personally identifiable information to mitigate privacy risks and incorporate privacy safeguards consistent with the Fair Information Practice Principles and Department privacy policy.

E. Data Access Review Council

The Data Access Review Council (DARC) is the DHS oversight and compliance body that reviews Departmental initiatives involving the internal or external bulk data transfer of personally identifiable information to support the Department's national and Homeland Security missions. The DARC advises on challenges related to bulk information sharing, including sharing in the cloud environment and the use of advanced analytical tools on DHS data.

The Data Access Review Council ensures bulk data transfers comply with applicable law and appropriately protect privacy, civil rights, and civil liberties of the individuals whose information is shared. As a discretionary matter, with the concurrence of other members, the Data Access Review Council may also review any matter referred by a member concerning the internal or external transfer of data (bulk or otherwise) or the development, execution, implementation, or operation of any Departmental information system.

Data Access Review Council initiatives primarily involve Information Sharing and Access Agreements with members of the Intelligence Community. Data Access Review Council membership includes the DHS Privacy Office, Office of Intelligence & Analysis, Office of Strategy, Policy and Plans, Office of the General Counsel, and Office for Civil Rights and Civil Liberties.

During the reporting period, the Privacy Office worked with U.S. Department of Homeland Security stakeholders and Intelligence Community partners on Information Sharing and Access Agreements or extensions for existing arrangements to ensure the identification and mitigation of privacy risks by completing privacy compliance documentation and analysis. The Privacy Office also monitors reports responsive to existing agreements' reporting provisions to ensure adherence to the agreements' terms and to ensure appropriate reporting and mitigation of any privacy incidents involving Department data.

F. Intelligence Product Reviews

Since 2009, the Privacy Office has reviewed the Office of Intelligence & Analysis' draft intelligence products intended for dissemination outside the Department and materials used to brief threat information to the Department's non-federal partners. In addition, the Privacy Office reviews requests for information related to source development, non-bulk information sharing,

and foreign disclosure. In conducting these reviews, the Privacy Office analyzes the products against Privacy Act requirements, the Fair Information Practice Principles, 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 the Office of Intelligence & Analysis's requests for review of requests for information and intelligence products. During this reporting period, the Privacy Office reviewed more than 1,156 intelligence products to ensure appropriate privacy safeguards were included in the final product, without impacting the analytic conclusions of the products. The Privacy Office also reviewed new or revised collection requirements drafted by the Office of Intelligence & Analysis to ensure compliance with guidelines that it not collect and maintain unauthorized or unneeded personally identifiable information.

G. 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, Canada, Poland, the Migration Five countries, Visa Waiver Program countries, and countries executing Preventing and Combatting Serious Crimes Agreements.

H. Working Group Participation

The Privacy Office addresses privacy 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 the Appendix.

I. Section Conclusion

During FY 2022, the Privacy Office provided targeted training and support to ensure compliance with privacy policy across the Department. For example, the Privacy Office provided training to fusion center privacy officers and analytical staff and hosted forums on handling and safeguarding Special Protected Classes information. The Privacy Office also provided specialized advice and guidance to safeguard privacy in information sharing and access agreements and initiatives involving the internal or external bulk data transfer of personally identifiable information to support the Department's national and homeland security missions. Additionally, the Privacy Office was an effective partner for the Office of Intelligence and Analysis in identifying and combating threats facing our nation while safeguarding privacy, without impacting the analytic conclusions of intelligence products.

V. Compliance & Oversight

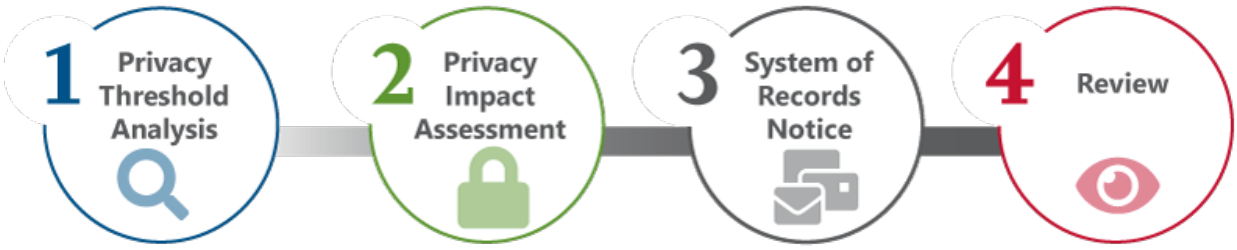
Through its compliance and oversight functions, the Privacy Office includes and enforces privacy safeguards in Department programs and operations. This section includes key metrics regarding compliance documentation and privacy incidents and provides updates regarding the Privacy Office's other compliance and oversight activities.

A. Privacy Compliance

The U.S. Department of Homeland Security's privacy compliance documentation process includes four primary documents: Privacy Threshold Analyses, Privacy Impact Assessments, System of Records Notices, and, when applicable, Privacy Compliance Reviews. Each of these documents has a distinct function in implementing privacy policy at DHS, and together they enhance transparency and accountability.

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 2: Privacy Compliance Process



The Privacy Office also conducts privacy reviews of the Office of Management and Budget 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[8] privacy reporting.

- At the end of the reporting period, 99 percent of the Department's Federal Information Security Modernization Act reportable systems requiring a Privacy Impact Assessment had completed one, and 100 percent of required System of Records Notices were completed.

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

1. Privacy Impact Assessments

The Chief Privacy Officer approved 30 new or updated Privacy Impact Assessments during the reporting period. Lists of all new or updated Privacy Impact Assessments can be found in the Privacy Office's Semi-Annual Section 803 Report. All unclassified Privacy Impact Assessments are posted on the Privacy Office website.

Table 2: New and Updated Privacy Impact Assessments, FY 2022

	New Privacy Impact Assessments	Updated Privacy Impact Assessments
FY 2022	16	14

2. System of Records Notices

The Chief Privacy Officer approved 13 System of Records Notices during the reporting period. Lists of all new or updated System of Records Notices can be found in the Privacy Office's Semi-Annual Section 803 Report. All System of Records Notices are posted on the Privacy Office website.

3. 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.[9] Data Integrity Board members include the DHS Inspector General, the Civil Rights and Civil Liberties Officer, the Chief Information Officer, and representatives of Components that are currently sharing information pursuant to a Computer Matching Agreement.[10]

The Data Integrity Board conducted its annual Computer Matching Agreement activity review and submitted the Department's 2021 Computer Matching Activity Annual Report[11] to the Office of Management and Budget in August 2022.

In 2022, the Department was a party to 11 Computer Matching Agreements that can be found on the Privacy Office website. During the reporting period, two of the agreements were extended for an additional year and six were renegotiated and will expire after eighteen months (unless extended).

[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 DIB, which must include the Inspector General. 5 U.S.C. § 552a(u)(2). Other members of the DIB are designated by the Chairperson.

[11] *See* https://www.dhs.gov/publication/computer-matching-agreement-activity-reports.

B. Privacy Oversight

1. Privacy Compliance Reviews

The Privacy Office exercises its oversight function under 6 U.S.C. § 142[12] in part by conducting Privacy Compliance Reviews.[13]

The Privacy Compliance Review framework emphasizes program involvement throughout the process. 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.

The Privacy Office oversight team periodically assesses the status of each Privacy Compliance Review recommendation and lists outstanding Privacy Compliance Review recommendations on the Privacy Office's website.[14]

2. 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 in collaboration with the DHS Enterprise Security Operations Center, Component Security Operations Centers, Component privacy officers, privacy points of contact, and DHS management officials.

During the reporting period, the Privacy Office continued efforts to prevent privacy incidents and ensure proper incident handling 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 conducting training (i.e., at new employee orientations, town halls, and during privacy events); and
- working with the Network Operations Security Center to develop a new enterprise incident database to enhance reporting and management of privacy incidents.

[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.

3. Incident Policies

The DHS Privacy Incident Handling Guidance[15] is the foundation of the Department's privacy incident response. The Department defines a privacy incident[16] 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 personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an unauthorized purpose. The term encompasses both suspected and confirmed incidents involving personally identifiable information, whether intentional or inadvertent, which result in a reasonable risk of harm to an individual.

4. Annual Privacy Incident Tabletop Exercise

During the reporting period, the Privacy Office planned and hosted the fifth Annual DHS Privacy Incident Tabletop Exercise from August 22, 2022 – September 1, 2022. The exercise was designed to practice and review important procedures, processes, concepts, and regulations in response to fictitious incident scenarios and to provide DHS professionals with an opportunity to connect and share best practices across the Department.

The exercise examined:

- Key DHS processes and procedures to address a privacy breach.

Roles and responsibilities in a privacy incident or a cybersecurity security incident involving personally identifiable information.

[15] *See* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.
[16] 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 maintained the term "privacy incident" to be consistent with other DHS incident types.

5. Incident Metrics

Table 3: Total number of privacy incidents by DHS Component for the period October 1, 2021 –September 30, 2022

Component	Privacy Incidents FY 2022
CBP	559
CISA	8
FEMA	15
FLETC	0
HQ	29
ICE	90
OIG	1
S&T	1
TSA	6
USCG	86
USCIS	122
USSS	4
Total	**921**

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.[17] The Chief Privacy Officer is then responsible for ensuring that appropriate remedial actions take place, including any required investigation and notification of the incident.

During this reporting period, 921 privacy incidents were reported to the DHS Security Operations Center.

6. Special Protected Classes – Unauthorized Disclosures

The Privacy Office and the Office for Civil Rights and Civil Liberties have implemented a notification process through which the two offices share responsibility for addressing incidents involving Section 1367 information. As discussed previously, release of personally identifiable information related to individuals in special protected classes could subject individuals to further harm and reprisal. The Privacy Office and Office for Civil Rights and Civil Liberties work together to ensure all incidents involving Special Protected Classes information are appropriately investigated, addressed, and resolved. Of the 921 total reported privacy incidents during this reporting period, there were seven reported incidents related to the unauthorized disclosure of Special Protected Classes information, four of which were confirmed incidents.

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

C. Section Conclusion

During the reporting period, the Privacy Office approved 30 new or updated Privacy Impact Assessments and published 13 System of Records Notices. Additionally, the Privacy Office continued its oversight efforts by assessing open Privacy Compliance Review recommendations, conducting the fifth Annual DHS Privacy Incident Tabletop Exercise, and handling 921 reported privacy incidents.

VI. Business Operations

The Business Operations Division ensures efficient Privacy Office operations, as well as the development and execution of internal and external communication strategies.

A. Operations and Workforce Support

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

- Leveraged intra-agency agreements to collect $4,505,693.33 in reimbursable funds, which enabled Components to use the Privacy Office's Freedom of Information Act and privacy support services contract vehicles. As a result, the Privacy Office provided surge staffing support to manage Component Freedom of Information Act backlogs and fund infrastructure and licensing costs related to Freedom of Information Act and Privacy Act processing technology.
- Closed an Office of Inspector General recommendation to develop and implement a department-wide process to monitor the completion of mandatory annual privacy training.
- Managed the operations of the Data Privacy and Integrity Advisory Committee and informed members about Privacy Office activities through the publication of a bi-monthly newsletter.
- Supported operations of the U.S. Department of Homeland Security Privacy Council and the Freedom of Information Act Council.
- Shared best practices for federal employees to protect their privacy online.
- Enhanced Privacy team communications through monthly Privacy Office town hall meetings and other events.
- Maintained a social media account for the Chief Privacy Officer.
- Detailed staff to support the Department's Southwest Border initiatives.

Additionally, the Privacy Office Business Operations Division conducted outreach, facilitated leadership development opportunities, provided skills training, and recruited diverse talent to support the Privacy Office's mission and advance its strategic goals.

B. Budget

In FY 2022, the Privacy Office's budget was $17,929,000. Sixty-eight percent of the budget supported Privacy Office personnel, compensation, and benefits and 20 percent supported contracts. The remaining three percent of the budget was spent on travel, supplies, and materials.

Notable FY 2022 highlights include:

- $2.6 million to fund 10 additional positions to meet the Department's operational and emerging efforts related to cyber intrusions, Domestic Violent Extremism, Artificial Intelligence, weapons of mass destruction, unmanned aircraft systems, advanced communications, autonomous things, advanced sensors and imaging technology, and COVID-19; and
- $3.5 million to procure and develop a modern Freedom of Information Act processing system to enhance processing, facilitate interoperability, and reduce administrative burden.

The Privacy Office maximized its resources by:

- allowing Components to purchase over $6,496,922 in Freedom of Information Act 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 $4,505,693.33 for infrastructure and licensing costs related to the web-based applications used to process Freedom of Information Act and Privacy Act requests.

C. Workforce

During the reporting period, the Privacy Office filled 7 additional positions, for a total of 56 federal employees. Newly filled FY 2022 positions include:

- Executive Director Strategic Privacy Initiatives;
- Special Policy Advisor & Director for Strategy and Integration;
- Management and Program Analyst;
- Administrative Specialist (Correspondence Specialist Privacy Office Executive Secretariat);
- Government Information Specialist (Privacy Policy);
- Management and Program Analyst (Intelligence Program Analyst); and
- Supervisory Government Information Specialist (Director for Compliance).

D. Staff Training and Development

To build a workforce that can contribute at its highest level, the Privacy Office encouraged its team and privacy and Freedom of Information Act professionals throughout the Department to seek development opportunities to further develop expertise and improve efficiency and productivity. The Privacy Office conducted privacy and Freedom of Information Act trainings and seminars to develop and maintain an effective, mission-focused, diverse, and knowledgeable workforce.

Privacy Office team members attended the following training and development opportunities:

- International Association of Privacy Professionals Global Privacy Summit;
- Federal Privacy Summit;
- Federal Privacy Bootcamp; and
- American Society of Access Professionals National Training Conference.

E. Section Conclusion

The Business Operations Division provided critical support for the Privacy Office's operations during the reporting period. In addition to assisting the Privacy Office with executing its budget, collecting funds for services, and filling vacancies, the Business Operations Team managed internal and external communications and advanced workforce excellence.

VII. Report Conclusion

In FY 2022, the Privacy Office made significant strategic and programmatic advances to achieve its mission to embed and enforce privacy safeguards and transparency in DHS activities while enabling the Department's mission. The Privacy Office will continue to build on these accomplishments in FY 2023 with the goal of ensuring that the Privacy Office continues to be a valuable partner to the Department and the public.

Appendix – Privacy Division Working Groups

Body	Description	Privacy Office Participation
Data Services Branch	The Data Services Branch 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 Data Services Branch through: -PTA submissions for each dataset targeted for onboarding, as well as updates to the Data Services Branch 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, and requestors must provide an articulated use consistent with the use or uses approved by the IT source system as a member of the Data Services Branch Working Group. -Approval of all bulk data transfers to ensure information sharing is governed by appropriate safeguards in accordance with the Fair Information Practice Principals through coordination with the Data Access Review Council
Data Stewardship Working Groups Data Stewardship Working Groups	The Data Stewardship Working Group is an outgrowth of the Immigration Data Integration Initiative Data Governance Working Group (IDII DGWG). The Data Stewardship Working Groups are responsible for each data set mission.	The Privacy Office is a member of several Data Stewardship Working Groups where the dataset(s) contains or leverages PII. Specifically, the Policy and Operations 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.
Risk and Resilience Policy Council	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	As mitigation activities develop, the Privacy Office will continue to focus on the safeguards around the use of Sensitive Personal Identifiable Information the impact on the individual, and compliance with privacy laws and policies.

	planning, guide investment, and foster collaboration.	
National Vetting Center Privacy, Civil Rights, and Civil Liberties Working Group	Privacy, Civil Rights, and Civil Liberties 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 Privacy, Civil Rights, and Civil Liberties Working Group and represents the Privacy, Civil Rights, and Civil Liberties Working Group as an *ex officio*, non-voting member of the National Vetting Center 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 National Vetting Center activities are conducted in a privacy-protective manner.
Targeted Violence and Terrorism Prevention Working Group	The Targeted Violence and Terrorism Prevention Working Group provides a forum for DHS Components and Offices to collaborate on targeted violence and terrorism prevention policies and strategies, and to develop cross-component targeted violence and terrorism prevention 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.