Data Privacy and Integrity Advisory Committee

November 7, 2023

Privacy Office

Protecting privacy while promoting transparency

AGENDA

I. Call to Order & Roll Call
II. Chair Opening Remarks
III. Chief Privacy Officer Updates
IV. Overview of the Privacy Office and DPIAC Tasking
V. Public Comment Period
VI. Meeting Adjourned

Call to Order & Roll Call

Sandy Taylor, Designated Federal Official

Opening Remarks

Lisa Sotto
Chairperson
Data Privacy and Integrity Advisory Committee (DPIAC)

Remarks to the Committee

Chief Privacy Officer Mason C. Clutter

Privacy Office Overview and DPIAC Tasking

Chief Privacy Officer Mason C. Clutter

Privacy Office MISSION and VISION

Our Mission

Promote and protect our shared values of privacy and transparency, while safeguarding the homeland.

Our Vision

Serve as a critical partner to our internal and external stakeholders in securing the homeland and protecting our values.

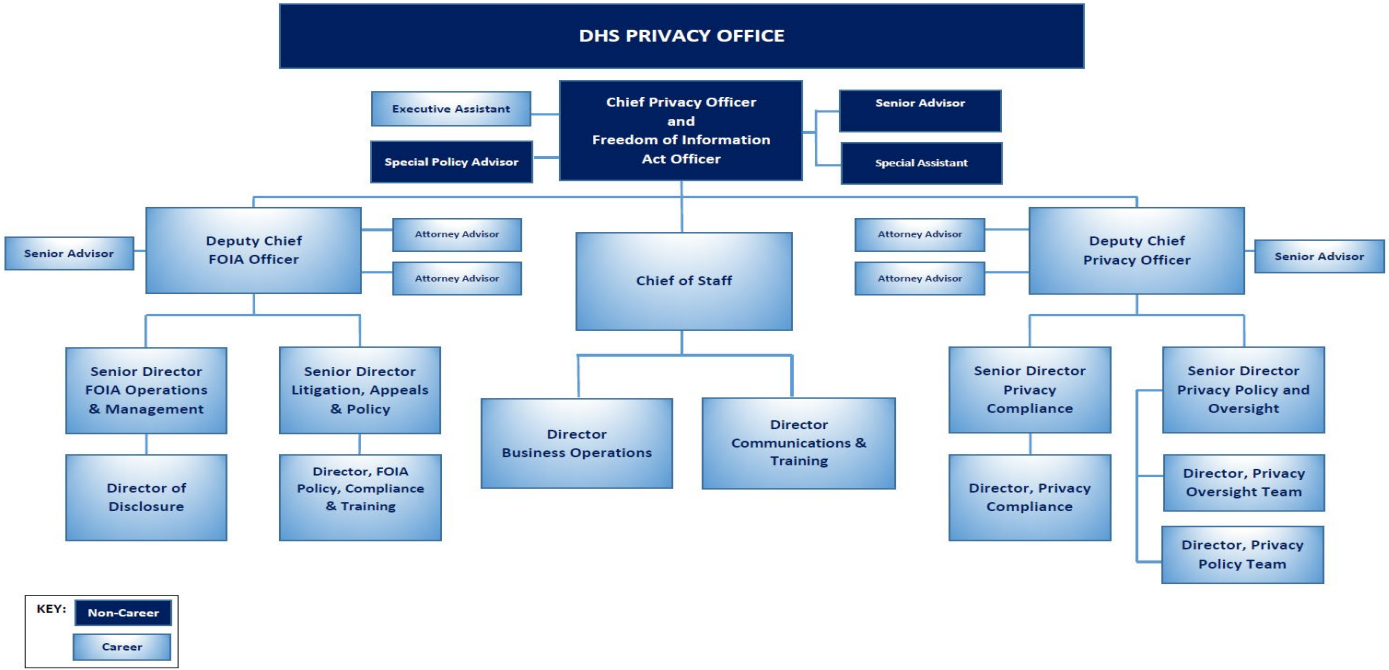
Privacy Office 2003

The Privacy Office's initial structure and staffing was focused on establishing and executing key DHS privacy and transparency responsibilities:

- Chief Privacy Officer;
- Chief of Staff and Director of International Privacy Policy;
- Chief Counsel to the Privacy Office (Office of the General Counsel);
- Director, Departmental Disclosure and FOIA;
- Director, Privacy Technology; and
- Director, Privacy Compliance.

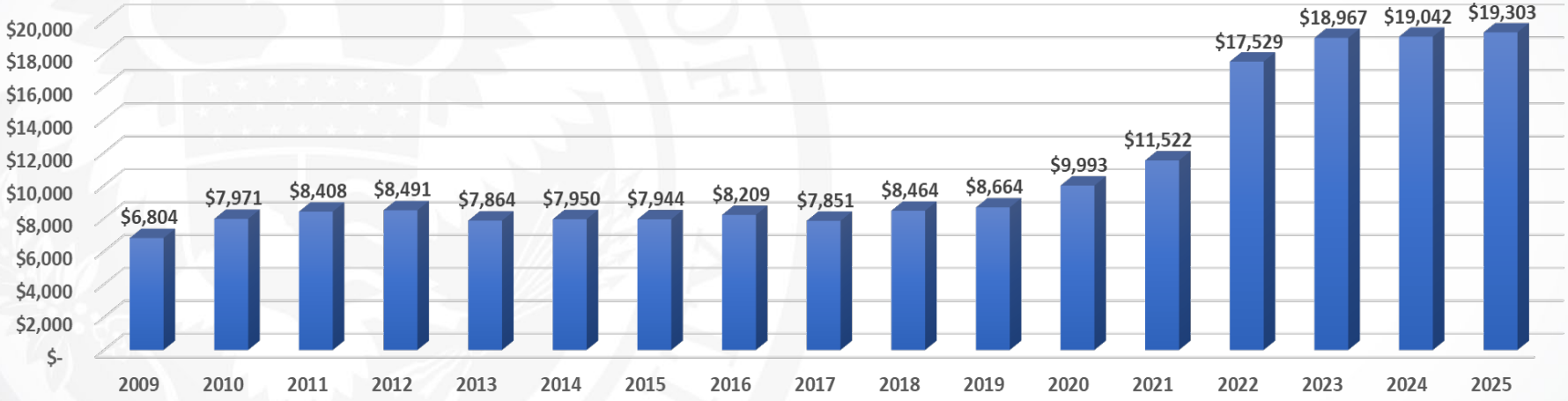
Additionally, there were three Component Privacy Officers across the Homeland Security Enterprise who reported to the Chief Privacy Officer and the Component heads: the US-VISIT Program, the National Cyber Security Division (within the Information Analysis and Infrastructure Protection Directorate), and the Transportation Security Administration.

Privacy Office Organization 2023



Privacy Office Staffing 2003-2025

Privacy Office Budget 2009-2025



Statutory Duties of the Chief Privacy Officer - 2003

Statutory responsibilities of the DHS Chief Privacy Officer are set forth in Section 222 of the Homeland Security Act of 2002 (6 U.S.C. 142):

- (1) assure that the use of technologies sustain, and do not erode, privacy protections;
- (2) assure that personal information in Privacy Act systems of records is handled in full compliance with fair information practices in the Privacy Act of 1974;
- (3) evaluate legislative and regulatory proposals involving personal information;
- (4) conduct privacy impact assessments; and
- (5) report annually to Congress on Dept. activities that affect privacy, including privacy complaints, implementation of the Privacy Act, internal controls, etc.

Statutory Duties of the Chief Privacy Officer - 2023

In addition to the initial statutory authorities established in 2003, pursuant to the *Implementing the Recommendations of the 9/11 Commission Act of 2007* (Public Law 110-53) the DHS Chief Privacy Officer received additional authorities and responsibilities:

- Section 802: Investigate and report on DHS programs and operations with respect to privacy.
- Section 803: Submit quarterly reports on: (1) number/types of reviews undertaken by the Chief Privacy Officer; (2) type of advice provided and response; (3) number/nature of privacy complaints received; and (4) summary of the disposition of complaints, reviews and inquiries conducted, and impact of Officer's activities.
- Section 804: Report Data Mining activities annually to Congress.

Governing Privacy Policies

2008	2011	2022
The Fair Information Practice Principles (FIPP): Framework for Privacy Policy at the Department of Homeland Security	*Privacy Policy & Compliance DHS Directive 047-01*	DHS Privacy Policy *Regarding the Collection, Use, Retention, and Dissemination of Personally Identifiable Information DHS Directive 262-16*
The FIPPs provide the foundational principles for privacy policy and guideposts for their implementation at DHS.	This policy applies throughout DHS governing the collection, use, maintenance, disclosure, deletion, and destruction of Personally Identifiable Information (PII) and any other activity that impacts the privacy of individuals as determined by the Chief Privacy Officer.	Also know as the "mixed systems policy" that, in addition to establishing privacy policy for Information and Technology Management, applies privacy safeguards to all individuals, irrespective of immigration status, in DHS "mixed" systems of records.

DHS Fair Information Practice Principles

DHS Privacy Policy

2007
Privacy Technology Implementation Guide

This establishes a general guide for technology managers and developers to integrate privacy protections into operational IT systems.

2008
Privacy Impact Assessments Privacy Policy Guidance Memorandum 2008 02

This Policy memorandum establishes and defines when the Chief Privacy Officer conducts a Privacy Impact Assessment (PIA) of a program, technology, or information collection at DHS.

2009
Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy Guidance Memorandum

The Policy constitutes the DHS Federal ISE Privacy and Civil Liberties Protection Policy to protected information, which the ISE defines as information about U.S. citizens and legal permanent residents that is subject to information privacy, civil rights, and civil liberties protections required under the U.S. Constitution and Federal laws of the United States.

2011
Privacy Act Amendment Requests Privacy Policy Guidance Memorandum 2011 01

This Policy memorandum establishes the policy throughout DHS to identify, process, track, and report Privacy Act requests for amendment of records

2011
Roles & Responsibilities for Shared IT Services
Privacy Policy Guidance Memorandum 2011 02

This Privacy policy establishes the Department wide approach to the roles and responsibilities accompany cross component sharing of IT services.

2011
Computer Matching Agreements and the Data Integrity Board Directive 262 01

This Policy establishes the DHS Data Integrity Board (DIB) and Department wide policy for engaging in and approving Computer Matching Agreements (CMAs).

Privacy Policy, cont.

2011
Privacy Policy & Compliance

This policy establishes privacy policy throughout DHS regarding the collection, use, maintenance, disclosure, deletion, and destruction of PII and any other activity that impacts privacy of individuals as determined by the Chief Privacy Officer.

2012
Research Programs and Projects

This policy establishes the privacy policy throughout DHS for privacy sensitive research programs and projects, except research conducted by the Office of the Inspector General.

2012
Privacy Policy for Operational use of Social Media

This policy establishes the privacy policy for operational use of social media throughout DHS.

Privacy Policy Instructions, Directives, and Memoranda

2012

Chief Privacy Officer Investigations

This Policy implements the Chief Privacy Officer's investigatory responsibility under 6 U.S.C. § 142 to address possible violations or abuse concerning the administration of DHS programs or operations affecting privacy.

2016

DHS Mobile Applications DHS Instruction 047 01 003

This Instruction implements privacy policy throughout DHS concerning for mobile applications that are developed by,on behalf of, or in coordination with the Department.

2017

Component Privacy Officers

This policy requires DHS Components appoint a Privacy Officer to oversee privacy compliance, policy, and oversight activities in coordination with the Chief Privacy Officer.

2017

Privacy Incident Responsibilities & Breach Response Team

This policy establishes responsibilities and requirements for responding to all privacy incidents/breaches;

and

Establishes the requirement for the Chief Privacy Officer to convene and lead a Breach Response Team (BRT) when a major privacy incident" has occurred, or at the discretion of the Chief Privacy Officer.

Privacy Policy, cont.

2017

Handbook for Safeguarding Sensitive PII

This Handbook provides best practices and DHS policy requirements to prevent a privacy incident involving PII/SPII during all stages of the information lifecycle.

2017

Privacy Compliance Review

This policy establishes Component Heads' responsibility to assist the Chief Privacy Officer in reviewing Component activities to ensure that privacy protections are fully integrated into Component operations.

2017

Privacy Incident Handling Guidance

The "PIHG" establishes policy throughout DHS for responding to privacy incidents/breaches.

2019

Social Security Number Collection & Use Reduction

This policy establishes requirements for the elimination of the unnecessary collection, use, maintenance, and dissemination of SSNs by DHS programs, systems, and forms;

or

the use of a unique alternative identifier to the SSN;

or

the use of privacy enhancing SSN alternatives when there are technological, legal, or regulatory limitations to eliminating the SSN.

2022

Collection, Use, Retention, and Dissemination of Personally Identifiable Information

This policy applies throughout DHS and implements the "mixed systems policy" that, in addition to establishing privacy policy for Information and Technology Management, applies privacy safeguards to all individuals, irrespective of immigration status, in DHS "mixed" systems of records.

DPIAC Tasking

- Assess where DHS Privacy has been, where it is now, and where it should be going, including:
  - DHS Privacy's mission,
  - role within the Department,
  - resources,
  - compliance structure (consistent with law and policy),
  - oversight framework,
  - authorities/delegations,
  - policies.
- Should adjustments be made to the Privacy Office based on the Department's evolving mission and reliance on technology and data?
- Consider new technologies and uses like artificial intelligence and machine learning, biometrics, commercial data, and publicly available information.
- Assess opportunities, mechanisms, and framework(s) for enhanced transparency; engagement with external stakeholders, experts, and advocates; and opportunities to solicit public input and feedback.
- Consider opportunities to solicit public comment and public events, including input from privacy experts and advocates.
- Consider private sector approaches and whether and how such approaches may be applicable to DHS and DHS Privacy.

Public Comment

THANK YOU!