DHS PRIVACY OFFICE

Guide to Implementing Privacy

Version 1.0

June 3, 2010

DEPARTMENT OF HOMELAND SECURITY

TABLE OF CONTENTS

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Purpose of this Guide

The purpose of the Department of Homeland Security (DHS or Department) *Privacy Office Guide to Implementing Privacy* (Guide) is to inform the Department, other federal agencies, and the public about how the DHS Privacy Office implements privacy at DHS. The Guide provides an overview of the DHS Privacy Office's functions and transparency into its day-to-day operations. This guide may be particularly helpful to federal privacy practitioners, as it not only describes the wide-ranging activities of the Office, but also explains how the office works to build a privacy culture at DHS. The Privacy Office's detailed Freedom of Information Act (FOIA) functions are described separately in Section 11.

1.2 Where to go with Questions

The DHS Privacy Office maintains a webpage (www.dhs.gov/privacy) where you can find Office reports and other guidance, as well as information on DHS privacy policy, public workshops, and other Privacy Office activities. If you have questions that are not addressed by the information in this Guide or on the DHS Privacy Office website, please contact the DHS Privacy Office by email at privacy@dhs.gov or by phone at 703-235-0780.

1.3 Other DHS Privacy Office Resources

The DHS Privacy Office publishes a number of resources regarding privacy implementation at DHS, including policy memoranda, official guidance, and workshop reports. This Guide summarizes many of the principles and activities included in these resources. A list of DHS resources is included in Appendix C. We encourage you to consult Appendix C for documents that address specific subjects or operational matters of interest to you, and to contact the DHS Privacy Office if you have questions regarding these resources.

2.0 OVERVIEW OF THE DHS PRIVACY OFFICE

2.1 DHS Privacy Office and the Chief Privacy Officer

The DHS Privacy Office is the first statutorily created privacy office in the federal government. The Office operates under the direction of the DHS Chief Privacy Officer, who also serves as the Department's Chief Freedom of Information Act (FOIA) Officer.[1] A complete listing of the DHS Chief Privacy Officer's responsibilities can be found on the DHS Privacy Office's website at www.dhs.gov/privacy.

[1] The DHS Chief Privacy Officer is appointed by the Secretary of Homeland Security.

The mission of the DHS Privacy Office is to preserve and enhance privacy protections for all individuals, to promote transparency of DHS operations, and to serve as a leader in the privacy community. The Office accomplishes its mission by:

- Requiring compliance with the letter and spirit of federal laws that protect privacy;
- Centralizing FOIA[2] and Privacy Act[3] operations to provide policy and programmatic oversight and to support operational implementation within the DHS components;
- Providing education and outreach to build a culture of privacy and adherence to the Fair Information Practice Principles (FIPPs) across the Department; and
- Providing transparency to the public through published materials, formal notices, public workshops, and meetings.

The activities of the Office serve to build privacy into departmental programs. The Office implements privacy laws as well as the numerous Executive Orders, court decisions, and Department policies that govern the Department's collection, use, and disclosure of personally identifiable information (PII). A listing of the authorities, through which the Privacy Office accomplishes its activities and mission, is contained in Appendix A.

2.2 Organization of the DHS Privacy Office

The DHS Chief Privacy Officer is supported by a number of directors and associate directors as well as support staff and contractors. The Office consists of operational teams including: International Privacy Policy; Departmental Disclosure and FOIA; Privacy Compliance; Privacy Policy (including Communications and Training); Privacy Incidents and Inquiries; Privacy Technology and Intelligence; and Legislative and Regulatory Analysis. See Appendix B for further information on the organizational structure of the Office.

2.3 DHS Component Privacy Officers and Privacy Points of Contact

Each DHS operational component has either a Privacy Officer or a privacy point of contact (PPOC).[4] The DHS Privacy Office works closely with component Privacy Officers and PPOCs to ensure that programs[5] in the component agencies identify privacy issues and

[2] Freedom of Information Act (5 U.S.C.§ 552).
[3] Privacy Act of 1974 (5 U.S.C.§ 552a).
[4] A PPOC is an individual who is responsible for privacy within his or her component, directorate, or major program, but is not a full-time Privacy Officer. In 2009, the Secretary of DHS directed the following operational components to have full-time Privacy Officers who report to the component heads: Federal Emergency Management Agency (FEMA), National Protection and Programs Directorate (NPPD), Office of Intelligence and Analysis (I&A), Science and Technology Directorate (S&T), Transportation Security Administration (TSA), U.S. Citizenship and Immigration Services (USCIS), U.S. Coast Guard, U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), and U.S. Secret Service.
[5] Programs within DHS components may also have a Privacy Officer or PPOC if a primary function of the program involves collecting, using, maintaining, or disseminating PII (e.g., The USCIS Verification Division, which administers the E-Verify Program, has a designated Privacy Officer).

work to address them. The Office coordinates regular meetings with component Privacy Officers and PPOCs, including a monthly privacy compliance meeting. In addition, the DHS Privacy Office compliance staff serve as liaisons to each component. The compliance liaisons facilitate outreach to the components through regularly scheduled meetings, coordination of privacy compliance activities, and by serving as a resource for component privacy staff in the event privacy issues arise.

2.4 DHS Data Privacy and Integrity Advisory Committee

The DHS Data Privacy and Integrity Advisory Committee (DPIAC) convenes quarterly to advise the Secretary of Homeland Security and the DHS Chief Privacy Officer on issues relating to programmatic, policy, operational, administrative, and technological issues within DHS that relate to PII, data integrity, and other privacy-related matters. Advisory Committee members represent a balance of relevant opinions on privacy from the public sector, private sector, academia, and the privacy advocacy community. More information about the DPIAC is available on the DHS Privacy Office website.

3.0 POLICY FRAMEWORK

The DHS Privacy Office has primary authority under Section 222 of the Homeland Security Act of 2002 for privacy policy at DHS.[6] Section 222 gives the Office plenary authority to ensure that the use of technologies sustains, and does not erode, privacy protections relating to the collection, use, dissemination, and maintenance of personal information, and to ensure that PII in information systems is handled in full compliance with the fair information practices set forth in the Privacy Act. All DHS personnel, including federal employees, independent consultants, and government contractors involved in DHS programs must comply with DHS privacy policy.

3.1 Management Directive

The *DHS Privacy Office Management Directive No. 0470.2: Privacy Act Compliance* (Directive) establishes the basis for DHS policy for Privacy Act Compliance. The Directive, which was issued in 2005, is currently being revised. The Directive requires that all employees be made aware of, and comply with, the Privacy Act and ensure that information about individuals is collected, maintained, used, and disseminated in accordance with the Privacy Act and DHS regulations. The Directive outlines the responsibilities of DHS personnel, including the DHS Chief Privacy Officer, component heads, component Privacy Officers, and program and system managers as they relate to compliance with the requirements of the Privacy Act and other federal privacy laws, regulations, and DHS privacy policy.

[6] *See* Sections 222(a)(1) and (a)(2) of the Homeland Security Act of 2002, 6 U.S.C. § 142.

3.2 Privacy Policy Guidance and Memoranda

The DHS Privacy Office implements the policies outlined in its Directive, as well as other federal laws and regulations, by issuing policies and procedures, policy guidance, and memoranda. These documents explain the criteria for collecting and using PII in a manner that furthers the Department's mission yet minimizes the impact on individual privacy. The DHS Privacy Office may engage working groups of DHS staff to collaborate on complex privacy issues, to achieve a consensus when developing policy guidance or procedures, and to enhance the transparency of DHS programs. Working groups generally include privacy and security experts from the Office and the various DHS components and programs. A list of all current DHS Privacy Office policies and guidance documents is included in Appendix C and available on the DHS Privacy Office's website. The website is routinely updated to reflect new or revised guidance documents and memoranda.

3.3 The Fair Information Practice Principles (FIPPs)

The DHS Privacy Office's privacy policies and implementation are based on eight FIPPs that are rooted in the tenets of the Privacy Act of 1974 and govern the appropriate use of PII. DHS uses the FIPPs as the policy framework to enhance privacy protections by assessing the nature and purpose of all PII collected to fulfill DHS's mission. The Office has established the FIPPs as the foundational principles for privacy policy and implementation at DHS.[7] This framework is used in conducting Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and reviews of rulemakings.

[7] *See* Privacy Policy Guidance and Memorandum No. 2008-01: *The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security*, a*vailable at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

The DHS FIPPs:

- Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of PII.
- Individual Participation: DHS should, to the extent practical, seek individual consent for the collection, use, dissemination, and maintenance of PII and should provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
- Purpose Specification: DHS should specifically articulate the authority, which permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- Data Minimization: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
- Use Limitation: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected.
- Data Quality and Integrity: DHS should, to the extent practical, ensure that PII is accurate, relevant, timely, and complete, within the context of each use of the PII;
- Security: DHS should protect PII (in all forms) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure; and
- Accountability and Auditing: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

3.4 Component-Level Policies

Component Privacy Officers and PPOCs develop component-level privacy policies as needed to reflect and further the mission of the component, ensuring that such privacy policies are consistent with DHS Privacy Office policies and the FIPPs. Such policies often address specific mission roles or programs. They also can inform development of DHS-wide policies. The Office reviews privacy policies and guidance developed by component Privacy Officers and PPOCs to ensure consistency in privacy policy across the Department.

3.5 Review and Comment on Federal Privacy Policy Development

In addition to departmental and component policies, the DHS Privacy Office may be asked to review proposed privacy-related documents submitted to DHS for comment by other federal agencies, including the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). The Office facilitates the review process by consolidating DHS component reviews from the component Privacy Officers and PPOCs and communicating those comments, together with its own analysis, back to the issuing entity.

The DHS Chief Privacy Officer actively participates on the Federal Chief Information Officer (CIO) Council Privacy Committee, the interagency organization of federal Senior Agency Officials for Privacy (SAOPs) and Chief Privacy Officers and has served as Committee Co-Chair since 2009. DHS Privacy Office staff also participates on subcommittees of the Privacy Committee, providing expertise that helps inform policy development and best practices across the federal government.

4.0 OVERVIEW OF PII HANDLING REQUIREMENTS

4.1 Minimizing and Protecting the Collection of PII

The DHS Privacy Office recognizes that collecting PII is integral to the operations and functions of the Department, its components, and programs. As a FIPPs principle, data minimization underlies all Office policies and procedures, which are designed to ensure that PII is collected only to the extent authorized by law and necessary to accomplish the Department's mission.

Through the Privacy Threshold Analysis (PTA), PIA, and SORN certification and re-certification process, DHS programs inventory, document, and publish their current holdings of PII and ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, complete, and reduced to the minimum necessary for the performance of a documented agency function.[8] DHS components and programs routinely inventory holdings of PII through the PTA recertification process or when a program's PIAs and/or SORNs are reviewed for ongoing accuracy. As part of this PII inventory review and compliance document recertification process, DHS programs will also assess their recordkeeping and disposal policies and practices as they pertain to holdings of PII.

4.2 Handling Sensitive PII

The DHS Privacy Office *Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS* (Sensitive PII Handbook)[9] sets standards for how DHS personnel should handle PII that requires stricter handling guidelines because of the nature of the data and the increased risk to an individual if his or her data were compromised. Sensitive PII is defined as PII which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security numbers (SSN), Alien Registration Numbers (A-Numbers), account numbers, medical information, and criminal history. Some information is sensitive because of its context. For example, a

[8] Refer to Section 5.0, *Privacy Compliance*, for more information on PTAs, PIAs, and SORNs.
[9] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_spii_handbook.pdf.

federal air marshal's name and address are sensitive as is a list of employees who have received poor performance ratings.

The Sensitive PII Handbook explains how to identify Sensitive PII, how to protect Sensitive PII in various formats (e.g., paper, electronic), and what to do when Sensitive PII is believed to have been compromised. The Sensitive PII Handbook also contains instructions on encrypting data as well as frequently asked questions on specific procedures to follow when protecting Sensitive PII.

4.2.1 Minimizing the Use of Social Security Numbers

DHS treats SSNs as Sensitive PII.[10] In an ongoing effort to minimize the use of SSNs at DHS, the DHS Privacy Office issued Privacy Policy Guidance Memorandum No. 2007-02*: Use of Social Security Numbers at the Department of Homeland Security* (June 4, 2007).[11] This memorandum addresses the collection, use, dissemination, and maintenance of SSNs and requires that DHS programs collect, use, disseminate, and maintain SSNs only when required by statute or regulation or pursuant to a specific authorized purpose. The Privacy Office encourages DHS programs to create their own unique identifiers in lieu of SSNs to identify or link information concerning individuals.

4.2.2 Managing Computer-Readable Extracts Containing Sensitive PII

OMB Memorandum 07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (OMB M-07-16) requires federal agencies to have a process in place to log all computer-readable extracts (CREs) from databases holding sensitive information and to verify each extract, including whether sensitive data has been erased within 90 days or its use is still required.[12] In response to this requirement, the DHS Privacy Office and Chief Information Security Office have issued *DHS Policy and Procedures for Managing Computer-Readable Extracts Containing Sensitive PII* (DHS CRE policy) which outlines DHS requirements for documenting, tracking, and validating CREs.[13]

The DHS CRE Policy permits personnel to create and use CREs only for authorized official purposes and to share CREs only as authorized by the Privacy Act and other applicable federal law and policy. DHS requires that CREs be appropriately secured during storage and transmission in accordance with *DHS Sensitive Systems Policy Directive 4300A* (DHS Directive 4300A) and the Sensitive PII Handbook. DHS also requires that ad hoc CREs, or non-routine CREs, be documented, tracked, and validated.

[10] *See* Section 1.1 of the *Sensitive PII Handbook*.
[11] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-2.pdf.
[12] *See* OMB M-07-16, Attachment 1, Section C. *Security Requirements.*
[13] [placeholder for url/citation once the policy is published]

4.3 Information on Non-U.S. Persons

Under the DHS Mixed System Policy,[14] DHS treats systems that collect, use, maintain, and/or disseminate PII of U.S. persons, Lawful Permanent Residents (LPRs), and non-U.S. persons (so called "mixed systems) as Systems of Records subject to the protections of the Privacy Act.[15] Under this policy, DHS components handle PII of non-U.S. persons held in mixed systems in accordance with the FIPPs. Non-U.S. persons therefore have the right to access their PII and the right to amend their records, absent an exemption under the Privacy Act; however, this policy does not extend or create a right of judicial review for non-U.S. persons.

4.4 Information Sharing

The DHS Privacy Office ensures that privacy is considered through review of intra-governmental and international information sharing agreements. The Office has developed, in collaboration with the DHS Civil Rights and Civil Liberties Office (DHS CRCL), *The DHS Federal Information Sharing Environment (ISE) Privacy and Civil Liberties Protection Policy*.[16] The Program Manager for the ISE required all relevant entities to prepare such privacy protection policies to implement ISE requirements ensuring that the information privacy and other legal rights of Americans are protected in the development and use of the ISE.

In addition to reviewing information sharing arrangements, the DHS Chief Privacy Officer serves as a voting member of the DHS Information Sharing Governance Board (ISGB) and the Office is also represented on the DHS Information Sharing Coordinating Council (ISCC). The ISGB is responsible for approving the Department's information sharing and collaboration strategy, establishing goals and priorities, and overseeing the implementation of the strategy across the components. The ISCC is responsible for facilitating the coordination of information sharing across the Department and serving as the coordinating and action body for Department-wide information sharing matters. The Privacy Office's presence helps ensure that privacy is considered throughout the development cycle of each information sharing initiative undertaken by the Department.

4.5 Securing DHS Information Technology Systems that Contain PII

The DHS Privacy Office works closely with the DHS Chief Information Security Officer (CISO) to ensure that privacy is considered in IT system security activities.[17] DHS Privacy

---

[14] DHS Privacy Policy Guidance Memorandum No. 2007-01: *Regarding Collection, Use Retention, and Dissemination of Information on Non-U.S. Persons, available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

[15] The Privacy Act provides statutory privacy rights to U.S. Citizens and LPRs but does not cover visitors or aliens.

[16] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_crcl_guidance_ise_2009-01.pdf.

[17] A DHS IT System is an IT system operated, controlled, or directed by the U.S. Department of Homeland Security. This definition includes information systems that other entities, including private sector organizations, operate on behalf of or for the benefit of the Department of Homeland Security. DHS Directive 4300A, Section 1.4.8.

Office staff attend DHS CIO and DHS CISO meetings to increase coordination and cooperation to secure PII within DHS IT systems.

The DHS CISO maintains DHS Directive 4300A and the *DHS 4300A Sensitive System Handbook* as the foundation for IT security for sensitive systems, including privacy sensitive systems, at the Department.[18] DHS Directive 4300A and its accompanying Handbook help support the Department's privacy compliance requirements by including privacy-related policies and responsibilities for management, operational, and technical controls. The DHS Privacy Office provides updates to DHS Directive 4300A as warranted.

4.6 Evaluation of DHS Intelligence Products

The DHS Privacy Office also helps to ensure privacy standards are preserved within DHS intelligence products. Office staff review products prepared by the DHS Office of Intelligence and Analysis (I&A) to identify possible privacy-related concerns before they are released. Together with colleagues in DHS CRCL, the Office plays a major role in establishing privacy protections within the intelligence activities of the Department.

5.0 PRIVACY COMPLIANCE

The DHS Privacy Office evaluates all new or proposed DHS information systems and programs for their impact on privacy. The Office is responsible for evaluating new technologies, programs, regulations, and legislation for potential privacy impacts, and for advising DHS senior leadership regarding implementation of corresponding privacy protections. The Office uses its compliance documentation tools – PTAs and PIAs – to identify and reduce the privacy impact of Department activities. In addition, the Office meets regularly with the DHS CIO, the DHS CISO, component program or system owners, and component privacy offices to discuss new initiatives and how privacy can be addressed from the beginning of program design.

5.1 Identification and Compliance Oversight

The DHS Privacy Office identifies programs that must go through the privacy compliance process through three main avenues: the Federal Information Security Management Act (FISMA) Certification and Accreditation (C&A) process,[19] the OMB Exhibit 300 budget process, and the Enterprise Architecture Center for Excellence (EACOE) process. Working with the DHS CIO and DHS Chief Financial Officer (CFO), the Office plays an

[18] DHS defines a Privacy Sensitive System (PSS) as any system that collects, uses, disseminates, or maintains PII. DHS Directive 4300A, Section 1.4.19.

[19] System C&A refers to the FISMA requirement for comprehensive testing and evaluation of the management, operational, and technical security features of an IT system and the official management decision that authorizes the operation of an IT system. DHS Directive 4300A, Section 3.9. For more information on the C&A process, please refer to NIST SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, available at* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

integral role by serving as a subject matter expert for reviews of new IT programs and new budget programs to identify privacy compliance issues.

5.1.1 FISMA Privacy Reporting

Privacy and information security are closely linked, and strong practices in one area typically support the other. Ensuring security of PII is one of the FIPPs. To that end, the DHS Privacy Office works closely with the DHS CISO to monitor compliance with the privacy requirements under FISMA. On a quarterly and annual basis, DHS reports to OMB its progress in conducting PIAs and issuing SORNs for IT systems that are required to go through the FISMA C&A process.[20]

5.1.2 OMB Exhibit 300s

In addition to working with the DHS CISO's Office, the DHS Privacy Office is responsible for reviewing all major IT program capital expenditures on an annual basis, prior to submission to OMB for inclusion in the President's annual budget. A DHS program's OMB Exhibit 300[21] must demonstrate, among other things, that a program's investment planning properly addresses privacy. The Office's review of the Exhibit 300 is both substantive and procedural, ensuring that each investment has the proper privacy documentation in place at the correct time.

The Office compliance staff work with each program manager to complete necessary documents and ensure that appropriate privacy protections have been incorporated into the program. The Office evaluates and scores each investment based on its responses to a standardized set of questions, and ensures that the appropriate documentation has been completed. To receive a passing score, either submissions must include the appropriate privacy documentation or the Office must determine the investment does not require privacy documentation. The Office works in close cooperation with the DHS CIO and the DHS CFO to ensure that DHS IT investments meet the established legal and policy standards set forth by DHS, OMB, and the Congress.

5.1.3 Enterprise Architecture Board

To ensure that privacy is considered at the beginning of every IT system's development, the Privacy Office sits on the DHS Enterprise Architecture Board. The Enterprise Architecture Board operates through the DHS CIO and performs substantive and strategic reviews of all requests for new IT initiatives through the EACOE. The Privacy Office sits on the EACOE and reviews each request for new technology to ensure that all DHS uses of technology sustain privacy protections.

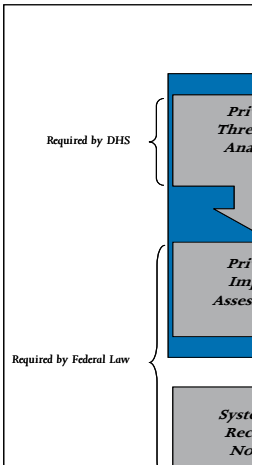
[20] See Section 12.3 for more information on FISMA reporting.
[21] *See* OMB Circular A-11, Section 300, *Planning, Budgeting, Acquisition, and Management of Capital Assets, available at* http://www.whitehouse.gov/OMB/circulars/a11/current_year/s300.pdf.

5.2 Compliance Documentation

The PTA, PIA, and SORN, which are described below, are the tools through which DHS assesses privacy in Departmental IT systems and programs and is able to track PII inventories. As part of the privacy compliance process, the DHS Privacy Office works with component Privacy Officers, PPOCs, program managers, system owners, and IT security personnel at Headquarters and DHS components to ensure that sound privacy practices and controls are integrated into the Department's operations. To assist those responsible for completing privacy compliance documentation, the Office has published official Department guidance regarding the requirements and content for PTAs, PIAs, SORNs, and Privacy Act (e)(3) Statements (disclosures required by Section (e)(3) of the Privacy Act to appear on documents used by the Department to collect PII from individuals to be maintained in a Privacy Act System of Records).[22]

5.2.1 PTAs

The DHS Privacy Office developed the PTA as part of the federal IT C&A process for systematically assessing the privacy impacts of IT systems. A PTA is required for every IT system, rulemaking, or program's use of PII at the Department. The PTA is performed to determine: (1) whether an activity involves PII; (2) whether a PIA is required; and (3) whether an existing SORN covers a particular collection, or if a new SORN is required. The PTA is also the means by which the Department ensures that privacy is considered in systems, that the DHS Privacy Office has reviewed an IT system as required under C&A, and that a security categorization has been assigned to a system based on the potential impact to the organization or individuals should there be a breach of security.[23]



The DHS Privacy Office also uses the PTA to formally document other decisions made by a program affecting privacy. For example, the Office can use PTAs to document and track a program IT system that collects SSNs from the public.

The program manager is responsible for completing the PTA in close cooperation with the component Privacy Officer or PPOC. Once the PTA is complete, the DHS Privacy Office reviews it and then engages in a detailed dialogue with the component Privacy Officer,

[22] These guidance documents are available on the DHS Privacy website and in Appendix C to this document.
[23] The Federal Information Processing Standards (FIPS) Publication 199 impact level – low, moderate, or high, is based on the sensitivity of the information maintained in the system. Systems that collect or maintain PII are designated at least "moderate" for security purposes. *See* FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* and OMB M-07-16.

program manager, information security officer, or PPOC as necessary. The DHS Director of Privacy Compliance determines whether a PIA or SORN is required based on the PTA. DHS PTAs expire and must be reviewed and re-certified every three years.

5.2.2 PIAs

The DHS Privacy Office conducts PIAs on technologies, rulemakings, programs, and activities, regardless of their type of classification, to ensure that privacy considerations and protections are incorporated into all activities of the Department.[24] A PIA assesses how PII is collected, used, disseminated, and maintained. It examines how the Department incorporates privacy throughout the development, design, and deployment of a technology, program, or rulemaking.

If a PIA is required, the program manager works closely with the component Privacy Officer to complete the PIA utilizing the DHS *Privacy Impact Assessments, Official Guidance* (PIA Guidance).[25] The PIA is intended to serve as a decision-making tool and should be used at the beginning of the design stage of a project and updated as needed to address significant changes in the project. Once completed, the PIA is sent to the DHS Privacy Office for review and approval by the DHS Chief Privacy Officer. DHS's PIA Guidance provides a detailed analysis for conducting PIAs and includes the *DHS Privacy Impact Assessment template*.[26] For additional information on the DHS Privacy Office's PIA policy, see DHS Privacy Policy Memorandum No. 2008-01: *DHS Policy Regarding Privacy Impact Assessments*.

The DHS Privacy Office conducts the following categories of PIAs: information technology; rulemaking; human resources;[27] national security systems; programs involving PII; privacy-sensitive technology; pilot testing; and, most recently, social media. Approved PIAs are published on the Office website unless they are classified, such as systems involving national security.[28]

5.2.3 SORNs

The DHS Privacy Office is responsible for managing the Department's SORN process. The Privacy Act requires federal agencies to issue SORNs for every system of records under their control that collects PII and from which information is retrieved by an

[24] Section 208 of the E-Government Act of 2002 requires federal agencies to conduct PIAs for any new or substantially changed technology that collects, maintains, or disseminates PII. The DHS Privacy Office also has its own statutory authority under section 222 of the Homeland Security Act to require PIAs. Finally, Congress may require PIAs for specific programs.
[25] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf.
[26] *Available at* https://dhsonline.dhs.gov/portal/jhtml/dc/sf.jhtml?doid=116936.
[27] Although the E-Government Act excludes systems that collect information solely about federal employees, DHS considers its employees' privacy to be no less important than the privacy of the public. This category of PIA focuses on HR systems that cover DHS Headquarters and/or affect two or more DHS components.
[28] *Available at* http://www.dhs.gov/files/publications/editorial_0511.shtm#1.

identifier.[29] A SORN is a legal document used to promote transparency and provide notice to the public regarding rights and procedures for accessing and correcting PII maintained by an agency on an individual.

To help facilitate the SORN process, the Office created a SORN template and published the DHS *System of Records Notice Official Guidance*.[30] DHS issues two types of SORNs: (1) DHS-wide SORNs that cover multiple systems of records with common subject matter or functions across the entire Department; and (2) component-specific SORNs that cover a system of records with subject matter or functions that apply to a specific component. A component-specific SORN may also cover a system of records that applies to more than one component but not to the Department as a whole. Each DHS component is responsible for identifying the system(s) of records for which it is responsible and completing the SORN process. Working with the component, the DHS Privacy Office determines if a new system can be covered by an existing SORN or if a new SORN needs to be drafted. The Office works closely with the project manager, the component Privacy Officer, and component counsel to draft new SORNs or update existing SORNs. The DHS Office of General Counsel performs a final review of each SORN. All SORNs are approved by the DHS Chief Privacy Officer prior to publication.

5.2.3.1 Publishing SORNs

The DHS Privacy Office is responsible for publishing all DHS SORNs. All SORNs must first be sent to OMB and to Congress for comment and are then published in the *Federal Register* to give the public notice and time to comment. To provide sufficient time to comment, a SORN (and Notice of Proposed Rule Making, if applicable) must be published in the *Federal Register* for 30 calendar days prior to the system becoming operational. If comments are filed, the Office works with the program manager and counsel to review them and publish a final rule. An updated SORN may be republished along with the final rule to address the comments.

5.2.3.2 Biennial SORN Review

The DHS Privacy Office works with DHS components to ensure that SORN reviews are conducted every two years following publication in the *Federal Register*. OMB requires each SORN to be reviewed every two years to ensure that it continues to accurately describe the system of records. Biennial SORN reviews include each system of records for which the agency has promulgated exemption rules pursuant to the Privacy Act, to determine whether such exemptions are still needed.[31] Biennial SORN reviews also examine the routine uses[32] or categories of approved sharing of information associated with

[29] 5 U.S.C. § 552a(a)(5) defines a Privacy Act system of records as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."
[30] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_sorn.pdf.
[31] *See* 5 U.S.C. §§ 522a(j)-522(a)(k) for a listing of specific exemption rules.
[32] The term "routine use" refers to the Privacy Act requirement that records can only be shared outside the agency for a purpose which is compatible with the purpose for which the record was collected. *See* 5 U.S.C. § 552a(a)(7). SORNs identify the routine uses for the public.

each system of records, to ensure that the recipient's use of such records continues to be compatible with the purpose for which the information was collected.[33] Only those SORNs requiring changes or updates are republished.

5.2.3.3 Retiring a System of Records

The Department notifies the public whenever a system of records is retired. A system of records (whether electronic, paper, or other form) must be removed from the Department's inventory when it is no longer needed by the Department. Eliminating such a system of records promotes the overall streamlining and management of DHS Privacy Act systems.

If the DHS Privacy Office determines that a system of records should be retired, the system manager and the component Privacy Officer or the DHS Privacy Office drafts a *Notice of Removal of a Privacy Act System of Records* (a "retirement notice"). The retirement notice summarizes what information system is being retired and why, followed by a brief description of what the system was originally designed to collect. The retirement notice is reviewed and approved by the component's legal counsel, the DHS Office of General Counsel, and the DHS Chief Privacy Officer. The notice goes to OMB for review before being published in the *Federal Register*.

5.2.4 Privacy Act (e)(3) Statements

The DHS Privacy Office has issued *Privacy Act Statements Guidance*[34] to provide instructions to DHS personnel on developing Privacy Act Statements required by subsection (e)(3) of the Privacy Act when collecting PII from the public.[35] Privacy Act Statements, or "(e)(3)" statements, are required on most forms (paper and electronic) that DHS uses to collect PII from members of the public, where the information will be entered into a system of records. These statements inform individuals at the time their information is collected what the legal authority for and purpose of the collection is, and how DHS will use this information. Privacy Act Statements also notify individuals as to whether providing the information requested is mandatory or voluntary and explain the consequences of failing to provide the information.

5.3 Computer Matching Agreements

The DHS Privacy Office reviews and clears computer matching agreements[36] for the Department and its components prior to submission to the DHS Data Integrity Board for

[33] From time to time DHS may choose to issue one annual comprehensive publication consolidating minor changes to SORNs. This requirement is distinguished from, and in addition to, the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the *Federal Register*.
[34] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guidance_e3.pdf.
[35] *See* 5 U.S.C. § 552a(e)(3).
[36] The Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. § 552a(a)(8)) amended the Privacy Act to require matching agreements before a department can match its data with another federal or state government, either as a recipient or the source of the data. A "matching program" is "any computerized comparison of two or more automated systems of records, or a system of records with non-federal records, for

the Board's statutory review and approval.[37] All DHS matching agreements must be approved by the Board.[38] Computer matching agreements are also required to include procedures governing the recipient agency's use of information and procedures on notification to individuals, information verification, record retention, and records security.

6.0 EDUCATION AND AWARENESS

6.1 Mandatory Training

The DHS Privacy Office is responsible for privacy awareness training for all new and current DHS employees and contractors. The Office provides instruction and materials on protecting PII and Sensitive PII in DHS systems. The Office developed a course entitled *A Culture of Privacy Awareness* as the required DHS annual privacy training course for all DHS employees and contractors. This course expands on basic privacy concepts initially presented in the new employee orientation and provides an understanding of the essentials of the Privacy Act and E-Government Act, including individual responsibility to use PII only for authorized purposes and to protect it from loss. *A Culture of Privacy Awareness* is offered on DHScovery, the web-based Learning Management System for DHS employees. The DHS Privacy Office provides copies of this training course to DHS components and to other federal agencies as requested. DHS has also recently mandated that all new headquarter employees attend the *DHS 101: Awareness Forum* within six months of hire. At the forum, the Office provides an overview of its role and how it interacts with the other components.

6.2 Supplemental Training

In addition to mandatory training, the DHS Privacy Office provides supplemental privacy training for the Department. For example, the Office conducts quarterly PIA training open to all DHS employees and contractors responsible for drafting privacy compliance documents. This hands-on course explains the PIA development and review process and offers an interactive forum for discussing issues that arise in the preparation of PIAs. In addition to quarterly PIA trainings, the Office conducts an annual one-day training regarding its compliance documents (PTAs, PIAs, and SORNs). This training is generally conducted in the late spring to coincide with the beginning of the OMB 300 budget process.

---

the purposes of establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applications 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, or recouping payments or delinquent debts under such federal benefit programs, or two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records." *See* 5 U.S.C. § 552a(a)(8)(A).

[37] The Chief Privacy Officer serves as the Chairperson of the DHS Data Integrity Board, which is responsible for approving and overseeing the Department's use of computer matching programs. *See* 5 U.S.C. § 552a(u).

[38] DHS is required, under OMB Circular A-130, to annually review each ongoing-matching program in which the agency participates in order to ensure that the requirements of the Privacy Act, OMB guidance, and any DHS regulations, operating instructions, or guidelines have been met.

6.3 Component Privacy Training and Awareness

In addition to the training programs offered by the DHS Privacy Office, a number of the component Privacy Officers and PPOCs offer privacy training and awareness programs tailored to meet the needs of their staff. Components may hold training sessions such as All Hands Training and Privacy Awareness Weeks, Privacy Awareness Days (including multiple one-hour sessions on protecting privacy), or poster campaigns promoting the protection of PII. The DHS Privacy Office also conducts training for components and programs, upon request, tailored to the issues most relevant to the component or program.

6.4 Fusion Center Training

Section 511 of the *Implementing Recommendations of the 9/11 Commission Act* (9/11 Commission Act)[39] requires that state and local fusion centers coordinate with the DHS Privacy Office and DHS CRCL to provide privacy and civil rights/civil liberties training for all state, local, tribal, and private-sector representatives working in fusion centers. To that end, the DHS Privacy Office, together with DHS CRCL, has taken a three-pronged approach to training for fusion centers.

- Train the Trainers Program - This training program educates appointed fusion center Privacy Officers about the scope and importance of their roles, and prepares them to develop and deliver their own state-specific training programs. Attendees of the two-day course receive training materials prepared by the Office and DHS CRCL, and are encouraged to continue engaging with the DHS Privacy and CRCL offices as they design their programs.
- In-Person Training – Each year the Office and DHS CRCL travel to a limited number of fusion centers to deliver the *Privacy Fundamentals for Fusion Center Professionals* training course, which provides an introduction to federal privacy protections and educates fusion center employees on (1) how to handle PII responsibly and consistent with the FIPPs and (2) how to recognize and address privacy incidents. This training is meant to supplement—not replace—the comprehensive, state-specific training delivered by each fusion center's Privacy Officer.
- Web-based Tool Kit – This tool kit provides a single source of information and useful resources about fusion center privacy and civil rights/civil liberties protections that Privacy Officers and intelligence analysts can use to understand and enhance privacy in their operations. The tool kit is available at http://www.it.ojp.gov/privacyliberty, and is updated regularly to include new guidance and other material relating to the fusion center privacy program.

[39] *See* Pub. L. No. 110-53, 121 Stat. 266.

6.5 DHS Privacy Office Staff Training and Certification

The DHS Privacy Office staff are required to maintain a high level of awareness of developments in privacy law, policy, and issues. Therefore, staff are encouraged to participate in national conferences and attend specialized training programs. The Office builds in-house expertise on current privacy issues by attending advanced courses and through extensive outreach to other federal agencies, privacy advocates, and other stakeholders.

Additionally, Office policy requires all staff to obtain and maintain the Certified Information Privacy Professional/Government (CIPP/G) certification offered by the International Association of Privacy Professionals (IAPP), a professional organization whose mission is to define, promote, and improve the privacy profession globally. To be recognized as a CIPP/G, privacy professionals must pass both the Foundation and CIPP/G examinations administered by the IAPP.

7.0 PRIVACY COMPLAINTS

The DHS Privacy Office ensures that DHS has procedures to receive, investigate, respond to, and provide redress for complaints from individuals who allege that the Department has violated their privacy. U.S. citizens, LPRs, visitors, and legal aliens may all file complaints or inquiries through a broad array of channels including telephone, email, facsimile, DHS redress programs,[40] and U.S. mail.

7.1 Managing Privacy Complaints

When the DHS Privacy Office receives a complaint, comment, or request for redress of a privacy issue, the complaint is entered into the Office's Complaint Tracking System (CTS) and is documented with the name of the complainant, type of complaint, and other pertinent data. Consistent with the quarterly reporting mandated by Section 803 of the 9/11 Commission Act, the DHS Privacy Office categorizes complaints as follows:

- *Process and Procedure:* Issues concerning process and procedure, such as consent, appropriate notice at the time of collection, or issues concerning notices provided in the *Federal Register*, such as rules and SORNs;
- *Redress:* Issues concerning appropriate access, correction, and redress;
- *Operational:* Issues related to general privacy concerns and concerns not related to transparency or redress; and
- *Referred:* The DHS component or the DHS Privacy Office determines that the complaint would be more appropriately handled by another DHS office or

[40] For example, the DHS Traveler Redress Inquiry Program (DHS TRIP) (*available at* http://ww6s1 113.54 191.69 Tm[( )] TJETBT/ovided in

component, another federal agency or other entity, and refers the complaint to the appropriate organization.

7.2 Disposition of Complaints

Dispositions of complaints are categorized in one of the three following categories:

- *Responsive Action Taken:* The DHS component or the DHS Privacy Office reviewed the complaint and a responsive action was taken. For example, for a travel screening-related complaint, an individual may be asked to provide additional information to distinguish himself from someone else, allowing the individual's information to be corrected.
- *No Action Required:* The DHS component or the DHS Privacy Office determined that the complaint does not ask for or require a DHS action or response. An example is a complaint regarding a published SORN that is no longer open to public comment.
- *Pending:* A DHS component or the DHS Privacy Office is reviewing the complaint to determine the appropriate response.

7.3 Coordination with the Office of the Inspector General (OIG)

Section 802 of the 9/11 Commission Act establishes formal requirements for the DHS Privacy Office to coordinate with the DHS OIG to investigate allegations of violations or abuse related to privacy within the Department. OIG staff members conducting privacy investigations must receive adequate training on privacy laws, rules, and regulations in consultation with the DHS Privacy Office. Section 802 requires that the OIG have an opportunity to decide whether to conduct investigations of alleged violations or abuse. If the OIG decides against opening an investigation, it refers the matter to the DHS Privacy Office for review.[41]

The DHS Privacy Office also works closely with the OIG to ensure departmental compliance with FISMA requirements. Each year, the OIG conducts a review of the Department's information security program and practices to determine whether they are adequate and to ascertain the extent to which DHS has made progress resolving issues cited in prior reviews. The DHS Privacy Office responds to privacy-related issues by recommending mitigation actions and providing status updates until those issues are resolved.

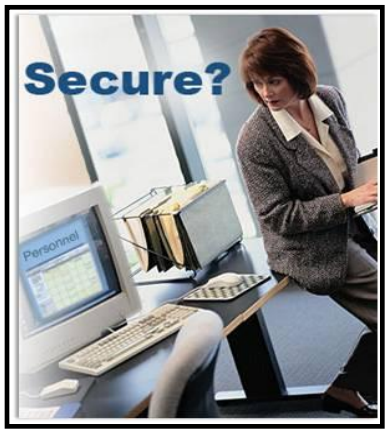
8.0 MANAGING PRIVACY INCIDENTS

The DHS Privacy Office is responsible for implementing and managing the Department's privacy incident and inquiries capture and response program. Working with the DHS CISO, the DHS Enterprise Operations Center (DHS EOC), and the DHS CIO, the Office

[41] 6 U.S.C § 142.

ensures that all DHS privacy and computer security incidents are identified, reported, and appropriately responded to in order to mitigate harm to individuals and to DHS-maintained assets and information.

8.1 Privacy Incident Handling Guidance



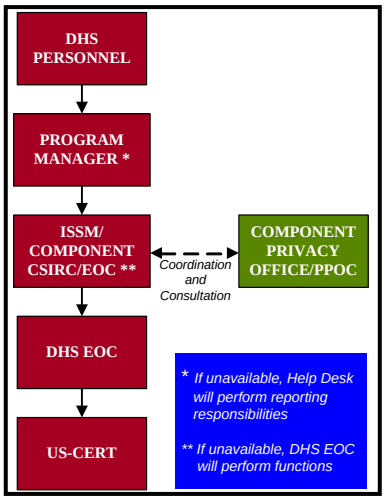
The DHS Privacy Office has developed and implemented *Privacy Incident Handling Guidance* (PIHG), which is the cornerstone of privacy incident policy, management, and response within DHS.[42] The PIHG informs DHS components, employees, and contractors of their obligation to protect the PII they are authorized to handle and how they must respond to any suspected or confirmed loss or compromise of PII. The PIHG defines the roles and responsibilities of personnel and management throughout DHS in responding to privacy incidents.

The PIHG uses OMB M-07-16 as the foundation for managing privacy incidents within the Department. In addition to OMB M-07-16, the PIHG also incorporates the framework for categorizing incidents described in Federal Information Processing Standards (FIPS) Publication 200 *Minimum Security Requirements for Federal Information and Information Systems*[43] and NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*.[44] While each privacy incident must be evaluated individually, the PIHG provides DHS offices, components, employees, and contractors with a set of guidelines for assessing a potential privacy incident and responding in a timely and appropriate manner.

The PIHG and the incident response processes have been incorporated into the DHS CISO Concept of Operations Plan as well as in the DHS Directive 4300A Policy and Handbook.

8.2 Privacy Incident Management

The DHS Privacy Office monitors new privacy incident reports through the DHS EOC Online Reporting System and notifies the component or program Privacy Officer or PPOC, Information System Security Manager (ISSM), and other component management officials of the incident by forwarding an initial incident report via email.[45] The DHS Privacy Office monitors through the DHS EOC online reporting system any action taken by components to remediate incidents, and provides guidance and assistance



[42] *Available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf.
[43] *Available at* http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.
[44] *Available at* http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf.
[45] Senior Department and component officials may be included on response teams involving moderate to high-impact privacy incidents.

to the DHS EOC Incident Analysts, the component EOC Analysts, and the component Privacy Officer or PPOC when required.

The DHS Privacy Office issues lists of outstanding (open) incidents to each component Privacy Officer or PPOC monthly for review, remediation, and closure. The Office reviews component and program requests to close open incidents and insures all PIHG requirements have been accomplished. Once all PIHG requirements have been met, the Office updates the DHS EOC Online Reporting System with its recommendation to close the privacy incident.

9.0 PUBLIC OUTREACH and TRANSPARENCY

9.1 U.S. Congress

The DHS Chief Privacy Officer appears periodically before congressional committees and subcommittees to address privacy issues or DHS policy positions. For example, the DHS Chief Privacy Officer may be asked to appear and explain steps the Office is taking to understand the privacy risks associated with a specific DHS activity or technology.

9.2 Workshops and Conferences

The DHS Privacy Office conducts public workshops to explore the policy, legal, and technology issues surrounding the intersection of privacy and homeland security. These programs include a broad range of experts and perspectives, including representatives of academia, business leaders, privacy advocates, legal experts, technologists, and policy leaders.

Workshops are publicly advertised in the *Federal Register* and on the DHS Privacy Office website and offer the public an opportunity to attend and to comment. Transcripts of the proceedings are published on the DHS Privacy Office website and generally accompanied by an official report.

DHS Privacy Office subject matter experts routinely participate in national conferences and specialized training programs. For example, DHS Privacy Office staff regularly participate in conferences of the IAPP and the American Society of Access Professionals (ASAP), the professional organization for federal government employees and private citizens working in the field of access to information under FOIA.

9.3 DHS Speaker Series

The DHS Privacy Office periodically sponsors a speaker series for DHS staff on privacy topics of interest. The speaker series provides an opportunity to discuss privacy issues with academic or policy leaders and other privacy experts in an informal setting.

9.4 Outreach with the Privacy Community

The DHS Privacy Office engages in outreach to advocacy groups and other groups with a particular interest in matters affecting privacy. The DHS Chief Privacy Officer hosts quarterly information sessions, entitled *Privacy Information for Advocates*, to brief advocacy groups on privacy issues of significance.

In June 2010, the DHS Chief Privacy Officer began sending out a monthly email to the privacy community summarizing recent topics of interest.

9.5 Leadership Journal

The DHS Chief Privacy Officer contributes periodically to the DHS Leadership Journal, [46] a forum for Homeland Security Secretary Janet Napolitano, and key DHS officials, to share news and insight, as well as The Blog @ Homeland Security.[47] Providing entries on these web-based outlets is an effective outreach tool that allows the DHS Chief Privacy Officer to quickly present his or her views to a large audience.

10.0 INTERNATIONAL ACTIVITIES

The DHS Privacy Office promotes international cooperation and understanding of privacy issues relevant to the Department's mission and operations. The Office's International Privacy Policy Group (IPP Group) educates the international community about DHS privacy practices and engages in dialogue through multilateral and bilateral partnerships. The IPP Group provides guidance within the Department and to other federal agencies on existing and emerging changes in privacy practices and global policy approaches, and provides advice to the Department and U.S. delegations negotiating international agreements related to personal information collection and sharing.

In support of the Department's mission, the IPP Group:

- Enhances the Department's information sharing opportunities with our international partners by providing educational outreach and leadership in areas such as privacy impact assessments and freedom of information;
- Interprets international data protection frameworks;
- Counsels the Department and other agency partners on existing and emerging changes in privacy practices and policy approaches globally;
- Engages in dialogues with international privacy authorities and bilateral partnerships, while also leveraging opportunities for dialogue in multilateral forums; and

[46] *Available at* http://journal.dhs.gov/.
[47] *Available at* http://blog.dhs.gov/.

- Provides counsel and oversight for international agreements related to personal information collection and sharing that impact the Department's mission.

10.1 International Information Sharing and Data Protection

Consistent with the Chief Privacy Officer's authority under Section 222 of the Homeland Security Act of 2002 and the DHS Mixed System Policy, the DHS Privacy Office reviews the Department's proposed information sharing agreements with international partners. The purpose of these reviews is to ensure that PII acquired or shared under these agreements is handled in full compliance with FIPPs. The Office works closely with the DHS Policy Office and DHS components engaged in international activities, contributing expertise in the planning stages of international information sharing arrangements with foreign partners, as well as in the negotiations and oversight of resulting agreements. The DHS Privacy Office IPP Group also serves as a resource to U.S. government agencies involved in cross-border information sharing arrangements.

10.2 Working with the International Community

The DHS Privacy Office works with its counterparts in Europe, Asia, and the Americas to promote understanding of how privacy issues are relevant to the Department's mission and operations. The FIPPs are the basis for privacy legislation in many countries. The IPP Group promotes confidence in DHS programs by demonstrating how these shared practices are incorporated into DHS systems and policies. The IPP Group also promotes reciprocity as an underlying principle for fostering the trust necessary for sharing vital information with ease, security, and transparency.

11.0 DEPARTMENTAL DISCLOSURE and FOIA PROGRAM

The DHS Privacy Office, through its Departmental Disclosure and FOIA staff (the Disclosure and FOIA Group), is responsible for administering policies, programs and procedures to ensure Department compliance with FOIA. Due to the synergies between privacy and FOIA, and in accordance with Executive Order 13392, *Improving Agency Disclosure of Information*,[48] former DHS Secretary Chertoff designated the DHS Chief Privacy Officer to serve concurrently as the DHS Chief FOIA Officer. The DHS Chief Privacy Officer's oversight of both privacy management and FOIA management allows for greater transparency of DHS operations.

DHS's policy is to implement both FOIA and the Privacy Act uniformly and consistently and to provide maximum allowable disclosure of agency records upon request. Requests processed under the Privacy Act are also processed under FOIA, and requesters are given the benefit of the statute with the more liberal release requirements.

[48] *Available at* http://www.fas.org/irp/offdocs/eo/eo-13392.htm.

11.1 Information on Submitting a FOIA or Privacy Act Request

The Disclosure and FOIA Group is responsible for drafting and implementing procedures for submitting FOIA and Privacy Act requests to the Department. The Group has developed and published detailed instructions for submitting FOIA or Privacy Act requests, which include limitations on requests, fees and fee waivers, response times, and where to send requests. Information on submitting FOIA and Privacy Act requests can be found on the DHS Privacy Office website dedicated to FOIA at www.dhs.gov/FOIA. The website also contains FOIA contact information.

In addition to information on submitting requests, the DHS FOIA website also contains a reading room of popular and frequently-requested departmental documents, as well as FOIA and Privacy Act statues and resources, many of which are referenced below.

11.2 Improving FOIA Operations

Executive Order 13392 directs agencies to ensure citizen-centered and results-oriented FOIA operations. In response, the Disclosure and FOIA Group drafted two DHS FOIA improvement plans that include concrete milestones, specific timetables, achievable outcomes, and metrics to measure success, while also focusing on particular DHS components with large backlogs.

As required by the Attorney General, the Disclosure and FOIA Group established backlog reduction goals for FOIA requests or administrative appeals pending beyond the statutory time period. These goals include overseeing all DHS components as they work toward eliminating their backlogs and providing components with monthly updates on their target completion rates.

In addition to the above-mentioned improvement plans, the Disclosure and FOIA Group is responsible for promulgating the Department's FOIA regulations.[49] These regulations outline FOIA requirements and responsibilities for DHS and its components and educate the public on FOIA requirements impacting DHS and proper procedures for filing a FOIA request. The regulations also provide detailed procedures and govern the way DHS and its components process FOIA Requests.

11.3 FOIA Guidance

The *Openness Promotes Efficiency in our National (OPEN) Government Act of 2007*[50] establishes a definition of "news media representatives" to ensure that FOIA offices consider the continuing evolution of methods of news delivery, such as freelance journalists, that distribute a "distinct work" to a public audience. The OPEN Government Act also directs that court-awarded attorneys' fees be paid from an agency's own appropriation, prohibits agencies from assessing certain fees if they fail to comply with

[49] 6 CFR Chapter 1 and Part 5.
[50] *See* Pub. L. No. 110-175, 121 STAT. 2524.

FOIA deadlines, and establishes an Office of Government Information Services at the National Archives and Records Administration (NARA) to review agency compliance with FOIA. The Disclosure and FOIA Group developed and issued Department-wide guidance regarding the implementation of the OPEN Government Act, highlighting both ways in which the Department was already compliant with the Act and necessary improvements.

11.4 Implementing New Administration FOIA Policy

The Disclosure and FOIA Group is responsible for reviewing and revising existing DHS FOIA policies and procedures to reflect changes in federal FOIA requirements. For example, the Office issued updates to DHS FOIA policies and procedures to reflect compliance with the Transparency and Open Government Memorandum for the Heads of Executive Departments and Agencies issued by the President on January 21, 2009[51] and pursuant to the Attorney General's March 19, 2009 FOIA Memorandum to the Heads of Executive Departments and Agencies.[52] These policies reversed FOIA guidelines that had been in place since 2001 and implemented a presumption of openness – the core tenet of FOIA.

In addition to revising policies and procedures, the Group issues memoranda notifying DHS components of any new FOIA requirements, and works with component FOIA offices to comply with new FOIA guidance. For example, on December 8, 2009, OMB released the Open Government Directive (OGD) to guide agencies in their implementation of President Obama's transparency agenda. The Disclosure and FOIA Group promotes compliance with the objectives of the OGD by working with components to ensure they devote adequate resources to their FOIA programs.

11.5 Intra-Departmental Compliance, Outreach and Customer Service

The Disclosure and FOIA Group is responsible for assisting DHS components with reducing the number of backlogged FOIA requests. The Group assists underperforming components with designing program improvements to decrease their backlogs by increasing productivity via personnel and technology. Improvements include contracting with outside entities to bring in additional personnel and implementing technology solutions that streamline the FOIA process.

The Disclosure and FOIA Group issues Department-wide guidance on the management of FOIA requests in an effort to ensure consistent responses throughout the Department. For example, the Group provides direction regarding which DHS components have responsibility in cases where files are shared between components, and coordinates Department-wide responses. Components actively participate in Department-wide FOIA initiatives to enhance responsibility and accountability, manage workload, and implement guidance provided by the Group.

[51] *Available at* http://edocket.access.gpo.gov/2009/pdf/E9-1777.pdf.
[52] *Available at* http://www.usdoj.gov/ag/foia-memo-march2009.pdf.

In addition to policy and program development activities, the Disclosure and FOIA Group is responsible for processing FOIA requests for DHS Headquarters programs that do not have FOIA offices, including the Office of the Secretary. The Director, Disclosure & FOIA serves as a liaison to DHS components, forwarding FOIA and Privacy Act requests seeking records those components maintain. The Associate Director of Disclosure Policy and FOIA Program Development offers FOIA and Privacy Act training during new employee orientation and to all DHS components on an as-needed basis to enhance FOIA officers' knowledge and expertise.

The Disclosure and FOIA Group represents the Department at quarterly meetings of the United States Department of Justice's (DOJ) Office of Information Policy (OIP) FOIA Officer's Homeland Security Information Group (FOHSIG), a working group convened by DOJ OIP to discuss FOIA issues that affect homeland security. The FOHSIG discusses pending litigation that may affect the federal government's ability to invoke FOIA exemptions to protect sensitive homeland security information, as well as procedural matters relating to homeland security.

12.0 REPORTING

The DHS Privacy Office issues a number of reports throughout the year. In most cases these reports are required by law and cover functions of the DHS Privacy Office as well as privacy-related activities within the DHS components.

12.1 Annual Privacy Report to Congress

The DHS Privacy Office submits an annual report to Congress on the activities of the Office, DHS components, and programs for the preceding year. The contents of the report vary from year to year but routinely address the following areas:

- Privacy-related activities of the Department;
- Specific privacy activities of the components;
- Technology updates;
- Privacy compliance;
- Privacy complaints;
- Internal education and training;
- Public outreach;
- Interagency privacy activities;
- International privacy activities;
- Reporting; and
- Privacy Act and FOIA Requests and Disclosures.

12.2 Annual FOIA Report to the Attorney General of the United States

As required by the OPEN Government Act of 2007, the FOIA and Disclosure Group prepares and submits the Department's annual report on FOIA activities and statistics to the Attorney General of the United States. Information in the report includes updates on the operations of the program as well as the number of FOIA requests received and processed for the year throughout DHS. The Annual FOIA Report provides a greater level of granularity including:

- Number of times the component relied upon each statutory specific exemption (e.g., b(3) exemptions);
- Average and median initial request and appeal response times;
- Request counts by response times (i.e. number of requests responded to within 0-20 days; 21-40 days, in 20-day increments up to 300 days and between 301-400 days);
- List of the agency's 10 oldest pending requests and appeals;
- Accounting of requests seeking expedited treatment; and
- Accounting of all fee waiver assessment requests.

12.3 Chief FOIA Officer Report to the Attorney General of the United States

Pursuant to the Attorney General's March 19, 2009 FOIA Memorandum to the Heads of Executive Departments and Agencies, the FOIA and Disclosure Group also prepares the Chief FOIA Officer Report to the Attorney General of the United States on steps DHS has taken to improve FOIA operations and facilitate information disclosure at DHS. The reporting requirements include steps the Department has taken to:

- Apply the presumption of openness;
- Ensure DHS has an effective system for responding to requests;
- Increase proactive disclosures;
- Greater utilize technology; and
- Reduce backlogs and improve timeliness in responding to requests.

The DHS Privacy Office published the first annual DHS Chief FOIA Officer Report on March 15, 2010.

12.4 FISMA Reporting

FISMA requires each federal agency to develop, document, and implement an agency-wide information security program.[53] On a quarterly and annual basis, the DHS Privacy Office reports to OMB its progress in conducting PIAs and issuing SORNs for IT systems that are required to go through FISMA C&A. The quarterly FISMA report includes statistics on outstanding and completed PIAs and SORNs for DHS systems that are operational or that are registered in the Department's FISMA inventory system. The Annual FISMA Report combines the PIA and SORN statistics and the data required for Section 803 Reports, as well as any additional data OMB may specify under the annual FISMA reporting requirements.

12.4.1 Section 803 Reporting

As required by Section 803 of the 9/11 Commission Act, the DHS Privacy Office submits quarterly reports to Congress covering the Department's privacy protection activities.[54] Each report includes information on: (1) the number and types of reviews undertaken by the DHS Chief Privacy Officer; (2) the type of advice provided and the response to such advice; (3) the number and nature of the complaints received by the Department for alleged violations; and (4) the disposition of such complaints.

The DHS Privacy Office includes statistics on the following documents and reviews in its Section 803 Reports:

- PTAs;
- PIAs;
- SORNs and associated Privacy Act Exemptions;
- Privacy Act (e)(3) Statements;
- Computer Matching Agreements; and
- Privacy protection reviews of information technology and program budget requests to ensure that privacy requirements and costs are identified and incorporated into budget plans.

Section 803 Reports also include a summary of the number of DHS employees who have completed mandatory or supplemental privacy training conducted by the DHS Privacy Office or the components.

12.4.2 Reporting on Privacy Complaints

In accordance with Section 803 of the 9/11 Commission Act and OMB M-08-09 *New FISMA Reporting Requirement for FY2008*, the DHS Privacy Office is required to report to Congress quarterly on the number and types of privacy complaints received throughout the Department. Privacy complaint statistics are also reported in the DHS Privacy Office Annual Report to Congress.[55]

---

[53] FISMA, 44 U.S.C. § 3541, *et.seq*.
[54] *Available at* http://www.dhs.gov/files/publications/editorial_0514.shtm#3.
[55] The Privacy Office's procedures for handling privacy complaints are described in Section 7.0.

12.5 Section 804 Data Mining Reporting

The DHS Privacy Office submits an annual report to Congress as required by Section 804 of the 9/11 Commission Act, entitled *The Federal Agency Data Mining Reporting Act of 2007*.[56] Section 804 reports describe DHS programs that satisfy the Act's definition of "data mining" in accordance with detailed reporting criteria required by the Congress.[57]

12.6 Biennial Matching Activity Report

The DHS Data Integrity Board collects data summarizing DHS matching program activities and reports on the matching activity data every two years to both the DHS Secretary and to OMB. The report includes the following information:

- The names and positions of the members of the Data Integrity Board;
- A listing of all DHS matching programs;
- For each matching program, a cost/benefit analysis or the reasons for the waiver of the cost/benefit analysis;
- A description of any matching agreement the Board rejected;
- A listing of any violations of matching agreements; and
- A discussion of any litigation involving the Department's participation in any matching program, and an explanation of the steps the agency used to ensure the integrity of its data as well as the verification process it used.

13.0 CONCLUSION

The DHS Privacy Office has built a robust privacy program by using a wide variety of policy, compliance, and education tools that together implement the FIPPs across the Department. Privacy considerations are woven directly into business processes throughout the Department to ensure that privacy is integrated into decision making from the very beginning. This has required substantial resources, and the end result has been the establishment of one of the leading privacy programs within the federal government. This Guide is intended to help others understand how the Office builds a privacy culture while furthering the mission of the Department.

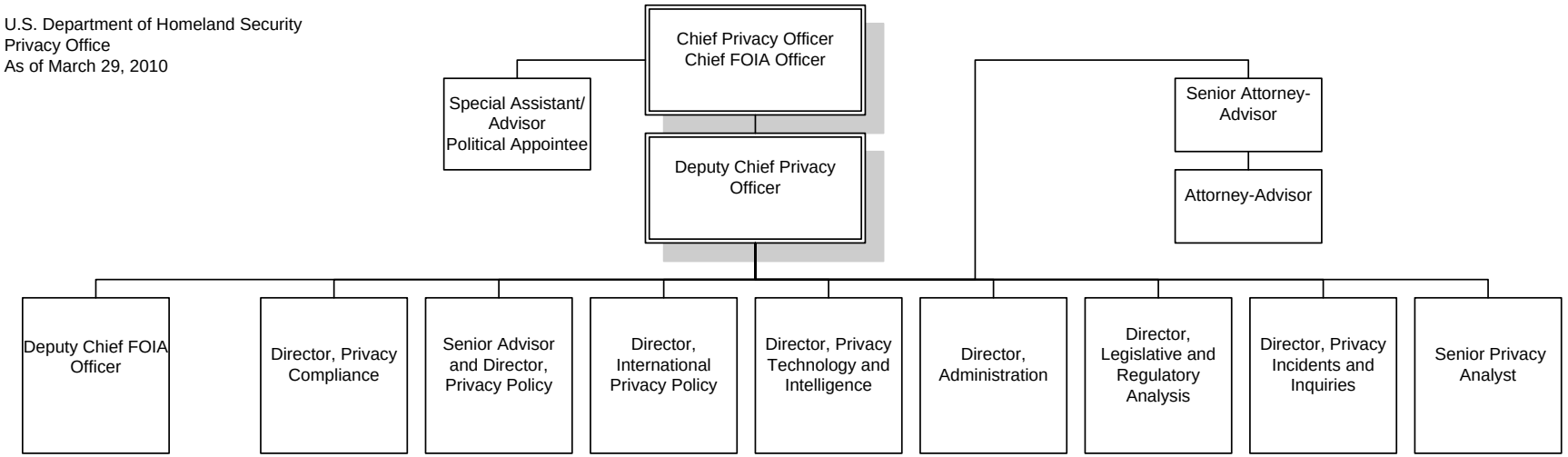
[56] *See* 42 U.S.C. § 2000ee-3.
[57] *See* 42 U.S.C. § 2000ee-3(b).

Appendix A: Authorities of the DHS Privacy Office

The activities of the Privacy Office serve to build privacy into DHS programs. The following is a framework of privacy laws through which the Privacy Office accomplishes its activities and mission:

- **Privacy Act of 1974, as amended (5 U.S.C. § 552a)**: Embodies a code of fair information principles that governs the collection, maintenance, use, and dissemination of personally identifiable information by federal agencies;
- **E-government Act of 2002 (Public Law No. 107-347, 116 Stat. 2899)**: Mandates Privacy Impact Assessments (PIAs) for all federal agencies when there are new collections of, or new technologies applied to, personally identifiable information;
- **Freedom of Information Act of 1966, as amended (5 U.S.C § 552)**: Implements the principle that persons have a fundamental right to know what their government is doing;
- **Section 222 of the Homeland Security Act of 2002, as amended (6 U.S.C. § 142)**: Creates the Chief Privacy Officer at DHS and delegates responsibilities to the DHS Chief Privacy Officer to ensure privacy and transparency in government are implemented throughout the Department;
- **Implementing the Recommendations of the 9/11 Commission Act of 2007 (Public Law No. 110-53, 121 Stat. 266)**: Amends the Homeland Security Act to give new authorities to the DHS Chief Privacy Officer.
- **Executive Order 13392 Improving Agency Disclosure of Information ():** Directs agencies to ensure citizen-centered and results-oriented FOIA operations; and
- **Office of Management and Budget (OMB) Memoranda** that specify privacy requirements and recommendations.

Appendix B: DHS Privacy Office Organization Chart



Appendix C: DHS Privacy Office Official Guidance and Policy Memoranda

Official Guidance

- Privacy Threshold Analysis Template (PTA), effective May 2008
- Privacy Impact Assessments (PIAs), effective May 2007
- System of Records Notices (SORNs), effective April 2008
- Privacy Act Statements ((e) 3) statements), effective April 2008
- Privacy Technology Implementation Guide (PTIG), effective August 2007
- Privacy Incident Handling Guidance (PIHG), effective September 2007
- Handbook for Safeguarding Sensitive Personally Identifiable Information at DHS, (SPII Handbook), effective October 2008

Policy Memoranda

- The Department of Homeland Security's Federal Information Sharing Environment Privacy and Civil Liberties Protection Policy, June 5, 2009
- DHS Policy Regarding Privacy Impact Assessments, December 30, 2008
- The Fair Information Practices Principles: Framework for Privacy Policy at the Department of Homeland Security, December 29, 2008
- Regarding the Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons, January 7, 2009 (as amended from January 19, 2007
- Regarding Use of Social Security Numbers at the Department of Homeland Security, June 4, 2007

For additional information on official guidance and memoranda issued by the DHS Privacy Office, or to review the content of the above listed documents, please visit the DHS Privacy Office website at www.dhs.gov/privacy.