The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

The Fair Information Practice Principles at Work

DHS issued Privacy Policy Guidance Memorandum 2008-01 on December 29, 2008 memorializing the Fair Information Practice Principles (FIPPs) as the foundational principles for privacy policy and implementation at DHS. The eight FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of personally identifiable information (PII). The FIPPs are embedded into DHS privacy sensitive systems, programs, and information sharing arrangements and are derived from the Privacy Act and other federal and international privacy guidelines. This document provides some typical examples of how the DHS Privacy Office oversees implementation of the FIPPs in the Department.

Transparency

DHS employs several means to provide transparency to the public of its activities and DHS privacy protections. DHS provides public notice of the collection, use, dissemination, and maintenance of PII through various mechanisms including: direct notice (commonly referred to as a Privacy Act e (3) statement) on forms used to collect information from individuals,; signage at U.S. ports of entry; and publication of privacy compliance documentation such as Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs). More broadly, DHS implements transparency by making its PIAs, SORNs, guidance, and other reports, including congressionally-mandated reports, available on the DHS Privacy Office website located at http://www.dhs.gov/privacy. In some instances, law enforcement or national security concerns prevent public disclosure of specific details of systems and programs. In these defined cases, DHS notifies the public of the exemptions for relevant systems. Even for these exempted systems, however, DHS reviews access requests on a case-by-case basis.

Individual Participation

DHS and its components have varied missions, including benefits administration, grants administration, border management, transportation security, cyber security, law enforcement, and national security. When programs carried out in pursuit of these missions require the collection of PII, DHS seeks to collect PII directly from individuals. If an individual believes a benefit was denied or some type of Departmental action (e.g., a referral to secondary screening) was taken as a result of an error in his information, that individual may, regardless of citizenship, seek access to, and, as appropriate, correct his information through the Freedom of Information Act (FOIA)/Privacy Act process. Furthermore, DHS developed the DHS Traveler Redress Inquiry Program (DHS TRIP) to be a single point of contact to handle questions and concerns about travel screening. An individual has the additional option of submitting a request for correction directly with the DHS Chief Privacy Officer. Recognizing that certain DHS functions are law enforcement or national security sensitive, DHS will not always collect information directly from the individual or permit access to and/or correction of records through the FOIA/Privacy Act process. In these cases, the Department provides notice through the relevant system Privacy Act exemption(s), and through response to related inquiries.

Purpose Specification

DHS articulates the legal authority that permits the collection of PII as well as the purpose or purposes for which the PII is intended to be used in its PIAs and SORNs. As part of the privacy compliance process, a program must be able to articulate the need for a particular collection of information with an appropriate legal authority and purpose justification.

Data Minimization

DHS seeks to minimize its collection of PII through its privacy compliance processes in two ways. First, the DHS Privacy Office works with the Office of the Chief Information Officer on the Paperwork Reduction Act process that seeks to minimize the collection of information, including PII from the public. Second, PIAs and SORNs require that data elements being collected are both relevant and necessary for the stated purpose of the system. DHS places a special emphasis on reducing the use of Social Security numbers (SSNs). DHS does not collect SSNs unless there is a valid authority for their collection.

Use Limitation

DHS limits its uses of PII to those that are permissible under law, and articulated in published PIAs and SORNs. Uses may include sharing both inside and outside of DHS. Within the Department, use of PII is limited to personnel who have an authorized need-to-know for the information. For external sharing, these uses are legally defined "routine uses," and must be compatible with the original collection and purpose specification. Absent a statutory requirement to disclose specific information, such routine use sharing decisions are made following a case-by-case review by the DHS Privacy Office to ensure a request meets the requirements. Sharing PII with external entities is done pursuant to routine uses articulated in published SORNs and may also be authorized by a written information sharing agreement, such as a Memorandum of Understanding, between the Department and the receiving agency.

Data Quality and Integrity

To ensure data quality, DHS collects information directly from the individual where practicable, especially in benefit administration functions. Recognizing data errors occur, DHS has implemented redress mechanisms that enable individuals to seek access and correction of their information through the FOIA/Privacy Act process, as described above. Travelers who experience difficulties may also seek redress through DHS TRIP.

Security

Since privacy and security are complementary, DHS Privacy Office works closely with the Office of the Chief Information Officer and the Chief Information Security Officer to ensure that security controls are put in place in IT systems that are commensurate with the sensitivity of the information they hold. Privacy requirements are built into the DHS Sensitive Systems Security Policy to safeguard PII from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction. By law, such systems must be certified as meeting relevant security standards. System and program managers are required to complete a Privacy Threshold Analysis, as well as a PIA and SORN, if applicable, before an IT system becomes operational.

Accountability and Auditing

DHS' privacy protections are subject to oversight by its Chief Privacy Officer and Inspector General as well as by the Government Accountability Office and the U.S. Congress. In addition to these oversight mechanisms, component privacy officers, system owners, and program managers implement accountability in their systems and programs through activities such as periodic review of audit logs to ensure that uses of PII are consistent with the purposes articulated for the collection of that information, as required by the Privacy Act. Further, as public documents, PIAs and SORNs not only demonstrate transparency but also serve as means by which the public can hold the Department accountable for its collection, use, and sharing of PII.

June 2011

Website: www.dhs.gov/privacy Email: privacy@dhs.gov Phone: 703-235-0780