The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
privacy@dhs.gov
www.dhs.gov/privacy

December 29, 2008

PRIVACY POLICY GUIDANCE MEMORANDUM

Memorandum Number: 2008-01

FROM: Hugo Teufel III
Chief Privacy Officer

SUBJECT: The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security

I. PURPOSE

This Memorandum memorializes the Fair Information Practice Principles (FIPPs) as the foundational principles for privacy policy and implementation at the Department of Homeland Security (DHS).

II. AUTHORITY

The FIPPs are a set of eight principles that are rooted in the tenets of the Privacy Act of 1974.[1] The Chief Privacy Officer's authority to use these principles as the framework for privacy policy at DHS is based upon Sections 222 (a)(1) and (a)(2) of the Homeland Security Act of 2002, as amended,[2] which authorize the Chief Privacy Officer to assume primary responsibility for DHS privacy policy, including (1) assuring that the use of technologies sustains and does not erode, privacy protections relating to the use, collection, and disclosure of personal information; and (2) assuring that personal information contained in DHS Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act.

III. POLICY

The FIPPs form the basis of the Department's privacy compliance policies and procedures governing the use of personally identifiable information (PII). These principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. DHS uses the

[1] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.
[2] Homeland Security Act of 2002, as amended, 6 U.S.C. § 142.

FIPPs to assess and enhance privacy protections by analyzing the nature and purpose of the collection of PII to fulfill DHS's mission and how the Department can best provide privacy protections in light of these principles.

IV. BACKGROUND

The FIPPs are a widely accepted framework that is at the core of the Privacy Act of 1974 and is mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The concept of defining principles to be used in the evaluation and consideration of systems, processes, or programs that impact individual privacy is not a new one. In his seminal work, *Privacy and Freedom*, published in 1967, Professor Emeritus Alan Westin identified a number of "criteria for weighing conflicting interests."[3] A few years later, an advisory committee of the U.S. Department of Health, Education, and Welfare (HEW) proposed similar principles.

The HEW advisory committee's report, entitled, *Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*,[4] was the result of the committee's look at the impact of computerization of information on privacy and included recommendations on developing policies that would allow the benefits of computerization to go forward, but at the same time provide safeguards for personal privacy. The backdrop surrounding the HEW report and the Privacy Act included several years of intense Congressional hearings examining the surveillance activities of the Nixon and J. Edgar Hoover era and the post-Watergate support for government reform. Flowing from the numerous abuses of power uncovered by Congress and the media during the early 1970's, the Privacy Act set out a comprehensive regime limiting the collection, use and dissemination of personal information held by government agencies. The Privacy Act also established penalties for improper disclosure of personal information and gave individuals the right to gain access to their personal information held by Federal agencies.

A number of European countries also began to build upon the HEW principles and individually enacted omnibus data protection laws. In 1980, the international Organization of Economic Cooperation and Development (OECD) codified its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[5] In 1995, a variation of these principles became the basis of the European Union Data Protection Directive. The FIPPs have also been agreed upon by member countries, including the United States, through a consensus and formal ratification process and form the basis of many modern international privacy agreements and national laws.

---

[3] These principles were included in chapter 14 of *Privacy and Freedom*, entitled "Restoring the Balance of Privacy in America." The Privacy Office has not adopted the notion of balancing privacy against other values because that paradigm results in a zero-sum outcome and privacy often is diminished at the expense of security.

[4] http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm

[5] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

As recently as 2004, the FIPPs were championed again by the United States in the development of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[6] The FIPPs principles have also formed the basis of many individual laws in the United States, at the both Federal and state levels, including the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, and the Children's Online Privacy Protection Act. Many states have incorporated these principles in their own state laws governing public records and in some instances private sector data as well. A number of private and not-for-profit organizations have also incorporated these principles into their privacy policies.

Section 222 of the Homeland Security Act of 2002, as amended,[7] which is the basis for the authorities and responsibilities of the DHS Chief Privacy Officer, also recognizes the significance of the FIPPs. This section calls on the Chief Privacy Officer to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with *fair information practices* as set out in the Privacy Act of 1974" (emphasis added). . Pursuant to Section 222, the Privacy Office has used the FIPPs to assess privacy when conducting Privacy Impact Assessments, issuing System of Records Notices, and developing privacy policy for the Department. The FIPPs provide the foundation of all privacy policy development and implementation at the Department and must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status.

V. THE FAIR INFORMATION PRACTICE PRINCIPLES

- Transparency: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).

- Individual Participation: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.

- Purpose Specification: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

---

[6] http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

[7] Homeland Security Act of 2002, as amended, 6 U.S.C. § 142.

- 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 practicable, ensure that PII is accurate, relevant, timely, and complete.

- Security: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

- 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.

The DHS Privacy Office, therefore, has adopted the FIPPs as its privacy policy framework and seeks to apply them to the full breadth and diversity of DHS programs and activities. Any questions regarding the application or implementation of these principles should be directed to the DHS Privacy Office at privacy@dhs.gov or (703) 235-0780.