Data Privacy & Integrity Advisory Committee
Draft: February 2, 2009

PUBLIC LETTER

Secretary Janet Napolitano
Acting Chief Privacy Officer John W. Kropf
Department of Homeland Security

This letter reflects the consensus recommendations provided by the Data Privacy and Integrity Advisory Committee to the Secretary and Acting Chief Privacy Officer of the Department of Homeland Security (DHS). The Committee's charter under the Federal Advisory Committee Act is to provide advice on programmatic, policy, operational, administrative, and technological issues relevant to DHS that affect individual privacy, data integrity and other privacy-related issues. The Committee deliberated on and adopted the recommendations set forth below during a public meeting held by teleconference on February 3, 2009.

This letter outlines certain key privacy issues currently facing the Department of Homeland Security that the Committee believes the new Administration should review. We recognize that efforts are underway on many of these issues and our intention is to highlight their importance. The letter reflects the consensus view of the members of the Committee.

Privacy Office Structure and Operations

- Structure of the Privacy Office. The Committee believes that the Privacy Office should remain a separate office within the Department of Homeland Security (DHS or Department), with the Chief Privacy Officer reporting directly to the Secretary. The Office should not be merged with the Office for Civil Rights and Civil Liberties, which the Committee understands serves a function that is different from that of the Privacy Office. Where the Privacy Office builds programs to effectuate privacy rights, the Civil Liberties Office focuses on community relations and civil rights. Although the offices should work closely together, they have somewhat different perspectives. It is important to have two different offices to address issues from their varying perspectives. The Chief Privacy Officer should be a person who is trusted by the Secretary as a member of the DHS senior management team. He or she should be someone who has a proven record of leadership and decisiveness, and who acknowledges the value of privacy as the foundation for a democracy. The Chief Privacy Officer should be a strategic thinker (not solely a functionary who knows the Privacy Act).

- The Freedom of Information Act. The Freedom of Information Act (FOIA) function should remain within the Privacy Office. Many of the requirements of the Privacy Act facilitate the front end of privacy, establishing appropriate restrictions on information collection and use, whereas FOIA facilitates the back end, providing access and redress. The access and transparency provided by FOIA are a critical part of the Privacy Office's mission.

- Component Privacy Officers. The Committee believes that each DHS component should have a dedicated, accountable privacy officer. Those individuals should report directly to the component head as advisors on privacy issues, with dotted line reporting to the Chief Privacy Officer. Examples of components that should have Privacy Officers are Customs and Border Protection, the National Protection and Programs Directorate, the Federal Emergency Management Agency, the Office of Intelligence and Analysis, the U.S. Coast Guard and the U.S. Secret Service. The Committee recommends that the DHS Privacy Office continue to foster effective reporting and regular communication between the Privacy Office and each component privacy officer to make the most effective use of these critical assets.

- Data Governance. Integrating the policies, procedures, and technologies of systems managed by the Chief Information Officer (CIO), Chief Information Security Officer (CISO) and Chief Privacy Officer is critical to limiting risk and raising confidence in information system functionality and integrity. At a minimum, the Committee recommends regular communications and cooperation between, and management support for the mutual goals of, the Chief Privacy Officer and CISO. The Committee encourages DHS to support holistic data governance.

- Training and Awareness. The Committee supports the Privacy Office's ongoing efforts to build a culture of privacy throughout DHS to include all DHS employees and contractors. Those managing and operating systems should be fully educated in the procedural requirements that support the policies described in the DHS privacy documents (e.g., SORNs and PIAs).

- Role of the Data Privacy and Integrity Advisory Committee. The Privacy Office should continue to look for ways to bring the Committee's expertise in privacy law, policy, technology and management to bear on critical issues facing DHS. The Privacy Office should engage the Committee early in the process of considering new issues and programs in order to maximize the Committee's value to the Department.

- Interoperability of DHS Systems. Technology systems that can exchange data require policy-driven standards and interoperable and auditable functional components, such as identity credentialing, authentication, access control and others for robust privacy and security protections. The Committee encourages DHS to continue to work toward policy and functional interoperability in the development of new systems and when making major modifications to existing systems.

- Data Integrity Initiative. A prerequisite for privacy protection, as well as for extracting value from our bits and bytes, is to safeguard the integrity of data. Continued focus on and commitment to data integrity can increase the usefulness to the Department of personal data and also help ensure that the Department is adequately protecting what needs protection. The Committee recommends that DHS launch an initiative, led by the Privacy Office, to develop a rigorous and methodical approach to data integrity.

- Privacy Protection Innovation. DHS should invest in research to develop new applications and technologies to facilitate the protection of privacy. Any such research and development activities should be staffed and supported by the Privacy Office, the Science and Technology Directorate, and other appropriate components of the Department. The relevant activities could include developing a research agenda under which to procure innovative research or request ideas though RFIs, grants and other mechanisms.

- International Relations. As the government looks to obtain data from international partners, coordination on privacy issues will be critical. The Privacy Office has a wealth of expertise in international privacy issues and should continue to take a leadership role in the negotiation of any DHS agreements involving the collection or sharing of personally-identifiable information (PII).

- The Privacy Act. The Privacy Act of 1974 has not kept pace with the evolution of technology and developments in how data is collected, used, shared and stored. To the extent the Secretary is asked to submit recommendations to Congress for making the Act more relevant and effective, the Committee recommends that the Secretary seek guidance from the Privacy Office staff, who are experts in applying the Act's provisions throughout the Department.

Current DHS Privacy Issues

- E-Verify. The Committee recommends that DHS eliminate or significantly reduce fraud vulnerabilities in the current E-Verify system. At a minimum, such reductions should occur before further expanding the mandated use of the system. The Committee has made recommendations on improving employer authentication in its Report No. 2008-2. The lack of procedures for authenticating the eligibility of employers to use the system creates a significant opportunity for fraud, which could result in legal residents and citizens becoming victims of identity theft.

- Credentialing Programs. DHS has many different credentialing programs aimed at specific groups of individuals. By virtue of their origins, each program has been managed by a different component of DHS or different people within the component. DHS should review these programs in light of the growing need for interoperability among them and the importance of having consistent privacy and security policies. The Privacy Office should have a role in developing best practices for these programs to foster the goals of interoperability and consistency.

- Border Searches and Seizures of Stored Digital Information. This is currently a highly visible and sensitive issue. While certain DHS components may have legal authority to conduct border searches, there is a significant difference between looking at paper documents and searching through the volume of digital information that can be carried by travelers. The Privacy Office should have a role in reviewing current policies and practices for searches and seizures of digital information and developing guidelines to integrate privacy protections into these processes.

- Comprehensive National Cybersecurity Initiative. The comprehensive national cybersecurity initiative (CNCI) and the CSIS report on Securing Cyberspace for the 44th Presidency stress the need to update the government's legal authority to protect and defend cyberspace in the U.S. Classified intelligence systems raise specific and sometimes significant privacy issues, including the conflict between transparency and redress. The Privacy Office should continue to be involved in the CNCI and its component projects.

- REAL ID: Despite the best efforts of the Privacy Office and the Committee, the final rule under the REAL ID Act does not fully address privacy and data security. The Committee has made recommendations for strengthening the rule in this regard in its Report No. 2007-01. The rule leaves states in the position of subjecting their residents' personal information to the vulnerabilities of the state with the weakest protections. Since the rule has not yet gone into full effect, given the absence of the reference databases, it should at least be reviewed and considered for revision to better address privacy and data security issues regarding the shared state data. In addition, the rule's provision allowing for the placement of unencrypted personal information in the machine-readable zone, which encourages inappropriate data collection and mission creep, should be reviewed and considered for revision.