INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

January 21, 2005

The Honorable Joshua Bolten
Director, Office of Management and Budget
Executive Office of the President
17th and Pennsylvania Avenue, N.W.
Washington, D.C. 20503

Dear Mr. Director:

This letter offers the comments and advice of the Information Security and Privacy Advisory Board,1 on Section 522 of the Consolidated Appropriations Act of 2005, Division H Transportation/Treasury, which provides for the establishment of statutory Chief Privacy Officers in Federal departments and agencies and prescribes certain actions to meet Federal government privacy management responsibilities.

The Board believes that this law is a significant step forward in three primary ways.

- it recognizes the increased importance of privacy management by the Federal government in support of the Privacy Act, other privacy statutes and OMB privacy guidance such as the privacy impact assessment provisions of the E-Government Act;
- it establishes agency focus and accountability for information privacy management, by mandating establishment of Chief Privacy Officer positions in Federal agencies; and
- it makes clear that information privacy, although related to information security, requires unique processes and technology support systems, dedicated agency focus, educational efforts, and accountability.

1 The Information Security and Privacy Advisory Board (ISPAB) was originally created by the Computer Security Act of 1987 (P.L. 100-35) as the Computer System Security and Privacy Advisory Board. As a result of Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act of 2002, the Board's name was changed and its mandate was amended. The objectives of the Board are (1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy; (2) to advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST; and (3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency and the appropriate committees of the Congress.. See http://csrc/nist.gov/ispab for more on the Board's operation and membership.

With respect to the audit and reporting requirements of Section 522, the Board recommends that OMB consider whether these requirements can be harmonized with other reporting requirements (such as those now required for privacy impact assessments) to the extent possible, especially where additional privacy specific reporting would be a logical extension of audit and reporting efforts already being undertaken by agencies. There is an obvious connection with the reporting and independent assessment required under the Federal Information Security Management Act, although the Board urges caution in merging the two requirements. Viewing privacy solely as a technology issue or as subordinate to security risks undercuts the necessity of considering privacy on its own merits. The two areas, privacy and security, are highly interrelated and often mutually supportive, but each requires its own focus. Similarly, while privacy concerns often arise in the course of discussions about deploying new technologies, they are separate interests. Changes in information practices affecting individual privacy are often but not always driven by technology.

In September 2002, the ISPAB issued a report on the effectiveness of privacy management by Federal Departments and agencies and offered a set of concrete and practical recommendations for improving government performance in this area. A copy of our report, "*Computer System Security and Privacy Advisory Board Findings and Recommendations on Government Privacy Policy Setting and Management,"* is enclosed.

Among the Board's four major categories of recommendations, three specific initiatives are particularly relevant to Section 522 and to its establishment of Chief Privacy Officers:

- identifying government-wide, standardized privacy requirements or requirements definitions which can reflect mandates set forth in the Privacy Act, other statutes and regulations, and assisting in determining where there are policy gaps or conflicts;
- establishing mechanisms to ensure that those government officials responsible for the protection of private information understand and can accommodate, to the extent permitted by statute and regulation, the needs for data sharing and data matching of law enforcement agencies seeking to enhance homeland security; and
- establishing a formal working relationship among privacy officials, information security officials, agency CIO's, and the records management community, each of which has a major role in managing government data and setting records management policies.

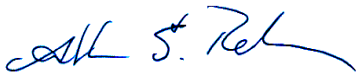
Although the Board has seen little progress to address its findings and recommendations, we believe that Section 522, properly implemented, can provide an enhanced management focus on privacy. It will also provide a favorable environment in which Federal agencies and departments with focused privacy responsibilities can cooperatively address information privacy issues which are best examined in a cross-government setting. To that end, Section 522 guidance issued by OMB would benefit from the inclusion of a core set of responsibilities expected of agency Chief Privacy Officers.

In the course of its continuing work on privacy, the Board has, over the past several years, examined the experience of Federal agencies, including the IRS and the Postal Service and, more recently the Department of Homeland Security, which have established chief privacy officers or privacy advocates. While broad conclusions about the effectiveness of those experiences would

be premature, anecdotal evidence suggests that each of those agencies has accrued significant benefits from those offices. The US-VISIT program in the Department of Homeland Security, for example, evinces a concern for the privacy of data subjects built into the design of the program that, the Board believes, can only enhance public acceptance. We trust that OMB will take account of the lessons learned from those agencies in its guidance on Section 522.

The Board would welcome the opportunity to support OMB as you examine models and to offer further recommendations for agencies as they implement Section 522.

Sincerely,



Franklin S. Reeder
Chairman

Enclosure: "*Computer System Security and Privacy Advisory Board Findings and Recommendations on Government Privacy Policy Setting and Management*," September 2002.

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-3357 *** Fax: 301/926-2733