

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

August 20, 2003

The Honorable Joshua B. Bolten
Director
Office of Management and Budget
725 17th Street, N. W.
Washington, D.C. 20503

Dear Mr. Bolten:

The Information Security and Privacy Advisory Board was established as a result of the Computer Security Act of 1987. The Board is charged to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy. The Board is also to advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget (OMB) on information security and privacy issues pertaining to Federal government information systems. The Board is an advisory committee operating in accordance with the Federal Advisory Committee Management Act.

Thus, as part of the Board's review of the security and privacy aspects of the Federal government's e-Government initiative, it has focused in particular on the e-Authentication initiative. Surveys show that the public's willingness to use the Internet and other modern technologies to obtain governmental information and services (e-government) is dependent, in large measure, on the public's confidence that those electronically-enabled systems and services can be trusted and that sensitive personal information about individuals will be safeguarded.

At the Board's June 10-12, 2003, meeting, we examined the issue of e-authentication models available for e-government services, hearing from representatives from the Liberty Alliance, Microsoft Passport, the National Research Council study panel which authored "Who Goes There? Authentication Through the Lens of Privacy," the Office of Management and Budget, the Government of Canada, the Center for Democracy and Technology (CDT), and the Electronic Privacy Information Center (EPIC). These presentations, while approaching e-authentication from different perspectives, nevertheless made clear the importance of establishing privacy policies and practices as mandatory components of technical models and systems being considered to support e-authentication services. What we heard from these expert speakers

suggested that information privacy principles, well understood and applied in public and private sector documents, and to a great extent mandated in the Privacy Act of 1974, must be actively applied in the development of requirements for government e-authentication systems and not retrofitted after design decisions have already been made.

In light of what we learned from these presentations and prior briefings from OMB and other Federal agencies representing work underway to plan and implement the e-government initiatives, it was unclear how the government has incorporated such legal requirements, policies and practices in the development of e-Government initiatives and in particular the e-Authentication initiative. For example, the government "E-Government Strategy," released in April 2003, includes only four references to privacy, and only one that is definitive, related to the development of Privacy Impact Assessments (PIAs) mandated by section 208 of the Electronic Government Act of 2002.

Given the importance of public understanding and acceptance of e-authentication systems, we recommend that OMB clarify how existing legal requirements, policies and practices have been incorporated into the policy, technical and legal architecture now being developed for e-Authentication.

The Board also recommends that OMB include requirements for addressing the privacy implications of e-authentication systems as part of guidance being developed for agency submissions of PIAs.

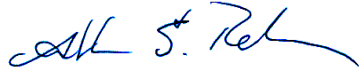
In bringing attention to these matters, the Board wishes to emphasize several issues addressed in our June meeting. A significant issue is the importance of minimizing authentication requirements where limited authentication will suffice or where anonymity is appropriate. This and other critical issues have recently been considered in the National Research Council (NRC) study, *Who Goes There: Authentication Through the Lens of Privacy*, and the report of the Center for Democracy and Technology's (CDT) Authentication Privacy Principles Working Group. We highly recommend that e-Government initiatives incorporate the principles and recommendations of these reports.

An additional issue, as the Board noted in its September 2002 report on privacy policy and management (<http://csrc.nist.gov/csspab/CSSPAB-Privacy-Report-2002-09.pdf>), is that changes in technology and information practices over the past thirty years require a review of the adequacy of the current legal framework for protecting personal information – in particular the Privacy Act of 1974. An example in the e-authentication context of why such a review is needed is the anticipated reliance by the Federal government on third-party systems for authentication. These third-party authentication systems are likely to result in massive databases, containing individual personal information, which may not be governed by the Privacy Act. Accordingly, it is important for government policy to: a) provide reasonable privacy rules including data minimization, with the databases not collecting more data than is needed; b) establish limits on data retention and re-use; and c) in general, adopt and implement the practices advocated by the Privacy Act and other guidance.

Under no circumstances should Federal government use of third-party systems for authentication be allowed to weaken the protections assured by the Privacy Act.

Thank you for the opportunity to share our findings.

Sincerely,

A handwritten signature in blue ink, appearing to read "Franklin S. Reeder". The signature is fluid and cursive, with a prominent initial "F" and a long, sweeping underline.

Franklin S. Reeder
Chairman