

INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

April 8, 2003

The Honorable Mitchell E. Daniels, Jr.
Director
Office of Management and Budget
17th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20503

Dear Mr. Daniels:

The Information Security and Privacy Advisory Board is a Federal advisory committee established by the Computer Security Act of 1987, as amended. The law directs the Board to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy in government systems. The Board is then to advise, among others, the Director, Office of Management and Budget and the Secretary of Commerce and to report its findings to the Secretary of Commerce, the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

At the Board's March meeting, we reviewed and discussed the National Strategy to Secure Cyberspace, issued in February 2003. Our review was preceded by a discussion with David Howe of the President's Critical Infrastructure Protection Board staff at the Board's December 2002 meeting. Mr. Howe briefed us on the process leading to the development of the final Strategy and invited us to submit Board comments. We submitted our comments on December 20, 2002, and are providing you with a copy.

The Board understands that it is the government's intent to treat the Strategy as a living document, that additional development of actions and recommendations will follow, and that the Strategy will evolve. The Board believes the following considerations are important to ensure that the Strategy's objectives are met as government moves forward to implement the document's actions and recommendations.

Implementation of the Strategy can benefit from existing government programs and capabilities. A number of important initiatives are already underway at the Department of Commerce's National Institute of Standards and Technology (NIST) that will provide significant and near-term support for key action and recommendations. For example, with respect to Action/Recommendations 3-1 and 3-3, NIST is already conducting security awareness seminars for the small business community.

Additionally, work underway at NIST, primarily in the Information Technology Laboratory, can directly support the Strategy's actions and recommendations. For example, these include commercial product security evaluation and validation, computer security and biometric standards development and testing, and programs to improve software quality. Increased direct funding for NIST programs should be given high priority.

With respect to Action/Recommendation 4-4, the Board questions the value of reviewing lessons-learned from implementation of the Defense Department's July 2002 policy requiring the acquisition of evaluated products. This policy has not been in place long enough to yield significant results. The Board also recommends that the broader review of the National Information Assurance Partnership (NIAP) include private sector participation in the examination.

The Strategy includes many recommendations for actions by the private sector to help secure cyberspace. In most instances the Strategy does not describe what Federal agencies can or should do to help advance such action through mechanisms routinely available to government. These include direct funding, indirect incentives such as creation of joint public-private forums and projects, or the use of existing regulations in support of cyber security.

As observed in the Strategy, a principal mechanism government has to compel action is its own purchasing power. It would be useful to require agencies to report periodically to OMB what they have done or are doing in their own procurement processes to purchase products and services in a fashion that promotes achieving the goals prescribed by the Strategy. Such guidance might be built into OMB's reporting process under the Federal Information Security Management Act (FISMA).

Regulatory authority already available to many agencies (such as FAA, NRC, EPA, DOL, FTC, SEC, FCC, Department of Health and Human Services, Department of the Treasury, and others) can be used to accelerate implementation of specific recommendations and actions made in the Strategy where appropriate. As the Strategy is implemented, it would be useful to ask agencies to report periodically to OMB and DHS what they have done or are doing with their regulatory authority to meet the goals prescribed by the Strategy. Agencies should also be asked to report whether changes to their regulatory authority are warranted to enhance their capabilities in this area.

As examples, compliance with the requirements of the Sarbanes-Oxley Act of 2002 could include the implementation of an effective information security program to help ensure the safeguarding of corporate information assets and the integrity of financial reporting. There are already precedents for this, as Department of Health and Human Services, Federal Energy Regulatory Commission, and the Nuclear Regulatory Commission, among others have sought NIST's advice with respect to information security implementations in support of regulations.

The Strategy raises larger issues arising from the increased policy and operational intersection between public and private sector critical infrastructure protection organizations and systems. Many of the Strategy's actions and recommendations point to a blurring of roles and responsibilities between what had been traditionally seen as national security and non-national security systems.

Recognizing the intent of the Computer Security Act of 1987, as reaffirmed by FISMA, this is an

issue that must be addressed more directly. Additionally, the Strategy minimally acknowledges the critical issue of information and citizen privacy and fails to provide specific actions or recommendations. The Board believes this must be addressed as well.

We thank you for your consideration.

Sincerely,

A handwritten signature in blue ink that reads "Franklin S. Reeder". The signature is written in a cursive style with a prominent initial "F" and a long, sweeping underline.

Franklin S. Reeder
Chairman

Enclosure