

COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

December 20, 2002

Mr. David Howe
Chief of Staff
Office of Cyberspace Security
Washington, DC 20500

Dear David:

Thank you for meeting with the Computer System Security and Privacy Advisory Board at the meeting earlier this month and briefing us on the draft Cyber Security Strategy. The Board was created under the Computer Security Act of 1987 (P.L. 100-35), and, among other things, has responsibility:

“to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy.”

As you suggested, we are sending you this letter to reflect the Board’s observations and recommendations on the September draft, most of which were shared with you at our meeting.

- Despite the fact that hardware and software reliability are fundamental to security, the draft Strategy makes only passing reference to reliability. The importance of reliability should be addressed and highlighted in the Strategy document, which should make clear that no unreliable system can be made secure. System reliability is important to security because a secure system relies upon the proper functioning of many elements, such as directories, relational databases, and other services. If those services are not reliably provided, then key security controls may cease operation. The Strategy should recommend actions to address this issue.
- Privacy is noted as a major concern in the draft Strategy, but there is very little in the form of substantive recommendations that explicitly address this issue. The Board has concluded a lengthy examination of privacy management in government systems and has issued a set of recommendations addressing the issues that arise when data are collected and shared in distributed environments across government agencies and with private sector companies. Such issues are very important to the business community, as industry will be expected, via Information Sharing and Analysis Centers (ISACs), to share vulnerability and threat information with the government. We recommend that the National Strategy address privacy with more specificity, from both personal and business perspectives, including action steps necessary to identify policy, management, and technical privacy controls which must be put in place to achieve a national cyber security system that with appropriate privacy controls.

- The Strategy generally takes a non-regulatory approach to providing cyber security direction to the private sector. However, in the Board's view, the Strategy should leverage the requirements of the Sarbanes-Oxley Act in prescribing management's responsibilities for establishing and maintaining adequate internal controls and procedures for financial reporting, which in turn require a secure and sound corporate technology infrastructure.

The Act is the most sweeping legislation affecting publicly traded companies since the Depression-era laws that form the basis for today's U.S. securities laws. . The Act significantly expands corporate reporting requirements and accountabilities, requiring executive certification of disclosure controls on a quarterly basis, and the filing of an internal control report with the annual financial report. The latter includes confirmation of management's responsibilities for establishing and maintaining adequate internal controls and procedures for financial reporting.

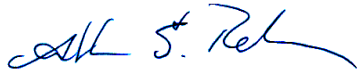
With today's dependency on information systems to support fundamental business processes, the adequacy of internal controls – including the completeness, accuracy, authorization and timeliness of transaction processing – is dependent in part on controls over information technology, including information security. Thus compliance with the requirements of the Sarbanes-Oxley Act of 2002 implies the implementation of an effective information security program to help ensure the safeguarding of corporate information assets and the integrity of financial reporting.

- The Strategy relies heavily on voluntary private sector action. However, experience to date suggests that, in the absence of regulatory requirements or direct financial support, this approach may be ineffective. To encourage widespread and effective industry adoption of the Strategy's recommendations, the Board believes that business incentives and benefits of various kinds need to be identified and incorporated in the Strategy. As one example, the financial services industry, through its BITS security initiatives, shows how individual businesses can upgrade their collective cyber security through cooperative action where common incentives are clearly understood. Incentives will vary from sector to sector and may be based on such factors as return on investment, reduced risk exposure, or even marketing value to participating companies. ISACs can prove useful in identifying specific incentives appropriate for companies in their industries.

The Board is at a loss to understand why the Office of Homeland Security has apparently decided not to release public comments that were received on the draft Strategy. We know of no other public comment process in which comments are not released, and find the assertion that commentators on proposed Federal policies have some expectation of privacy to be curious since the invitation to comment did not assert any such expectation, nor did the Web site. We do not doubt the sincerity of your Office's commitment to make the process of developing the strategy open and transparent, but are concerned that releasing only a summary of comments will needlessly undermine public confidence. We therefore urge you to reconsider that decision. In particular, if the Office of Homeland Security assured commentators that their responses would not be released, we encourage you to seek their permission to release their comments and to make all comments on future iterations public as well.

Once again, the Board is most appreciative of your willingness to share your views with us. We look forward to continuing the dialogue. We particularly applaud the commitment in the initial draft Strategy to make the Federal government a model for cyber security in its critical systems. The Board stands ready, consistent with its charter, to provide whatever advice and that you may require in pursuit of our shared goal of improving the level of security in Federal information systems.

Sincerely,

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

Franklin S. Reeder
Chairman