COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987

June 17, 1999

Mr. Raymond Kammer
Director, National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 1000
Gaithersburg, MD 20899-1000

Dear Mr. Kammer:

Thank you for your letter of November 16, 1998, noting topics on which you think the Computer Systems Security and Privacy Advisory Board (CSSPAB) could provide assistance.

The list is challenging, and over the last few years, the CSSPAB has explored aspects of them all at various times. During our meeting this month we devoted substantial time to discussing whether and how we could add value to each. Of necessity, our response needs to be consistent with our capabilities, resources and statutory mission; namely, to be alert to and call attention to privacy and security issues arising from the use of information technology by Federal agencies, and to provide advice to you and the Secretary of Commerce on those issues and report our findings to OMB, NSA and the Congress.

Security Metrics: In our discussions, we paid particular attention to the first topic on security metrics and reference data sets. It is a fundamental question that underlies many of the other topic areas. Metrics for security operate at many levels, ranging from detailed measures of device performance, to systems measures, to metrics for evaluating the contributions of a security program to enterprise-wide organizational goals. In our view, any fruitful discussion of the contribution of metrics to security implementation, as well as metric research program, must look at the entire span of measures.

Not much is yet well understood about security metrics, particularly at the higher, more general level. Yet this is where the need is greatest, both in the government and private sector. It is our view that an invitational symposium/workshop be held under the auspices of NIST, which would draw together government, industry, and academic security experts to explore the problem, and to create both a short and long term research agenda.

The workshop could be held at NIST next spring, perhaps in conjunction with the Board's spring meeting. The workshop would be designed to encourage leaders of government and industry to recommend specific metrics that might then be developed and could not only indicate the effectiveness of security processes and technologies but

Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-3696 *** Fax: 301/926-2733

also measure risk reduction. The results of the workshop should be reported in proceedings to government and industry for comment and refinement, with the view that the metrics can be used universally by the IT community to better assess and value the contributions of security toward enabling critical functions and infrastructures. The final workshop report could be published by NIST as a technical bulletin.

We also have been examining and will continue to work on aspects of the other issues that you have raised.

Identification of Top IT Security Research Issues: There have been many efforts at this task lately, notably the National Research Council, the Office of Science and Technology Policy, and the President's Commission on Critical Infrastructure Protection. We are examining and evaluating these in light of the most critical needs for security.

Federal Agency Improvement: As your letter notes, the Board has devoted substantial time over several years to this fundamental question. We have, at times, sent recommendations to NIST and the Commerce Department, and expect to do so in the future. The Board feels that fiscal support of investments in security of Federal systems, particularly in the non-defense civil sector is woefully inadequate to the task. This is true not only at the agency level but also at NIST, which has major responsibility to provide help securing civil sector federal information systems. The problem will grow even more severe as government agencies struggle to respond to directives from the Government Paperwork Elimination Act and various administration initiatives to exploit new information technology for improved and automated service delivery, information access and electronic transactions.

Privacy in the System Life-Cycle: We have a subcommittee of the Board looking at new issues of privacy as agency collection of personal data continues to expand and as they attempt to provide direct access and services over the Internet.

Thank you for your interest in and support of the work of the Board. We look forward to continue working with you on these critical issues.

Sincerely,

Willis H. Ware

Willis H. Ware, PhD
Chairman