INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

July 22, 2015

Dr. Willie E. May
Under Secretary of Commerce for Standards
and Technology
Director, National Institute of Standards and
Technology

Dear Dr. May:

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB or Board). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board, and amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002. The statutory objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

The OPM breach reminds us how important data risk management is in the federal enterprise. Agencies collecting, storing, and communicating national security, civilian, or commercial data need to have an inventory of which of their programs involve managing data that meet a threshold of high sensitivity.

This principle emerged again in the Board meeting on June 11, when we heard about a proposed rule by the Department of Commerce Bureau of Industry and Security (BIS) that would implement a licensing regime for exports of intrusion and surveillance technology. The proposed rule would require applicant companies to submit technical data to BIS for evaluation against the export control criteria.

The authority of the government to collect, store, and transmit sensitive commercial data confers responsibility on the agency for establishing and implementing stringent data security controls on

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

the implementation of their regulatory authority. The success of the program and of the commercial sectors being regulated depends on protecting that sensitive information.

This responsibility and the implied asset inventory process further require the agency's data security and program management offices to implement data security controls after evaluating program operations, sensitive data to be protected, and associated risk profiles.

It was clear during our briefing that such communication and awareness does not currently support the implementation of the BIS export control program. While the fundamental principles are well established in FISMA requirements, we are compelled to highlight the OPM breach as a marker for a future in which sensitive commercial information could be the next victim in a long string of security lapses in the government enterprise.

We recommend that the US Department of Commerce review this internal risk management process, especially for the export control program. ISPAB would appreciate hearing at its next meeting October 21, 22 and 23, 2015, the steps being taken to protect critical commercial information.

Sincerely,

Peter Weinberger, Ph.D.
Chair
Information Security and Privacy Advisory Board