INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

March 30, 2012

The Honorable Jeffrey Zients
Acting Director, US Office of Management and Budget
Washington, DC 20502

Dear Mr. Zients,

I am writing to you as the Chair of the Information Security and Privacy Advisory Board (ISPAB). The ISPAB was originally created by the Computer Security Act of 1987 (P.L. 100-35) 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. One of the statutory objectives of the Board is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At the Board's meeting of February 1-3, 2012, we discussed the state of computer operating systems used by Federal agencies, and the security risks posed by agencies' continued reliance on unsupported systems. Based on the Board's discussion at that and prior meetings, we are writing to suggest the Administration issue a straightforward policy to address this risk:

Outdated (e.g., unsupported) computer operating systems should be phased out.

This would have a significant positive impact on the cyber security posture of Federal agencies, and would demonstrate security leadership by example from the government.

The Board believes this action would support a number of other recommended cyber security actions. One such action involves implementation of best practices identified by the National Security Agency (see http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf) include running a modern 64-bit operating system. Much of the government, including parts responsible for security, does not follow this practice; for example, continued use of Windows XP by many agencies is not consistent with this best practice. Microsoft data shows that XP gets infected at a rate almost 10 times greater than a modern 64-bit system (see http://www.microsoft.com/security/sir/keyfindings/default.aspx#!section_4_2).

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

We recognize that transitioning from outdated operating systems would incur near-term costs, but these costs are inevitable and coming soon. For the XP example, as of April 8, 2014, Microsoft support will end (see http://windows.microsoft.com/en-US/windows/products/lifecycle), and there will be no more software updates, including for security. Continuing to use XP after that date will magnify security risks and associated mitigation costs, considerably. Timely, well-planned migration will also allow for appropriate attention to configuration management and testing prior to deployment to help ensure legacy applications continue to function.

Because of ever advancing threats, the risks of continuing to use obsolete (and soon unsupported) software are unacceptable. Further, at a time when those in the public and private sectors are looking to the US Government for advice on how to protect their systems, the Government should focus on minimizing its own vulnerability to maintain credibility as a purveyor of cyber advice.

There would be an immediate and significant benefit from implementing this policy. The gain in replacing outdated operating systems with more current versions that employ modern security techniques may be larger than that coming from the Trusted Internet Connections (TIC) program, continuous monitoring, or wider implementation of Homeland Security Presidential Directive (HSPD)12 - worthwhile programs in their own right, but without the broad and relatively fast impact that could be achieved through operating system upgrades.

The Board appreciates the opportunity to provide views on this important issue. We welcome further discussion at the Administration's discretion.

Sincerely,

Daniel J. Chenok
Chair, ISPAB

cc: Steve VanRoekel, Administrator of E-Government and Information Technology and CIO, OMB
Howard Schmidt, Cybersecurity Coordinator, National Security Council,
Mark Weatherford, Deputy Undersecretary for Cybersecurity, DHS
Patrick Gallagher, Director, NIST