INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

January 14, 2014

The Honorable Sylvia Mathews Burwell,
Director
Office of Management and Budget
Executive Office of the President
Washington, DC 20502

Dr. Patrick Gallagher
Under Secretary of Commerce for Standards and Technology
Director, National Institute of Standards and Technology

Dear Ms Burwell and Dr. Gallagher:

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. 100-235) as the Computer System Security and Privacy Advisory Board. The charter was subsequently amended by Public Law 107-347, The E-Government Act of 2002, Title III, The Federal Information Security Management Act (FISMA) of 2002, Section 21 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-4) and renamed it the ISPAB. The statutory objectives of the Board include identifying emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy.

At the Board's December 19-20, 2013 meeting we reviewed the NIST cryptographic standards development program in light of recent trust and confidence concerns raised in some press reports. The Board recognizes NIST Information Technology Laboratory's (ITL) long and successful history in the development and evolution of consensus-based cryptographic standards for use in private sector and federal non-national security systems. Over the decades, NIST has convened wide global cross-sections of stakeholders from government, academic, and industry communities with a stake in robust encryption. The NIST standards development program has always had broad participation by community representatives and results have been widely recognized and employed because the development of cryptographic standards is transparent, inclusive, and open. Over time, this process has generally earned trust and confidence globally in the implementation of encryption technology developed through consensus-based standards making. This well-understood process is foundational for ensuring widespread adoption, trust, and security.

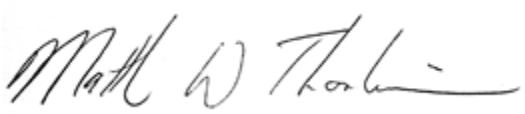
Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007

NIST has also subjected its encryption standards development process to periodic evaluation to understand what improvements can be made, and senior staff used the occasion of the latest ISPAB meeting to brief the Board about the evaluation process and solicit advice. This is a laudable demonstration of NIST's active stewardship of open standards development and a commitment to continuous improvement.

The Board commends NIST's adherence to the inclusive and transparent standards development principles that have sustained the effectiveness and credibility of NIST's standards mission. We strongly support NIST's process review to ensure that any recent or future developments do nothing to compromise those principles or discourage the active engagement of the stakeholder community that NIST serves. The Board also compliments NIST's interest in exploring new institutional partnerships to build on the credibility of its program, and we particularly encourage continued engagement with, and expanded outreach to, the academic community.

The Board looks forward to continuing work with NIST in order to ensure long-term trust and confidence in the development of cryptographic standards.

Sincerely,



Matt Thomlinson
Chair
Information Security and Privacy Advisory Board