INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

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

April 20, 2016

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.

At the Board's meeting on March 24, 2016, we heard from representatives of NIST on plans to update FIPS-140. The plans seemed to rely on including ISO 19790 in the revised standard. The Board agrees that FIPS-140 needs revision, and concurs on the general advisability of having NIST standards align with other international standards. The Board is unable to endorse this specific use of an international standard, as ISO 19790 is not generally available. A quick web search shows that ISO is charging CHF 178[1] just to look at this ISO standard, which is more than $180.

The Board believes that essential cryptographic standards, such as FIPS-140, should be generally available to the public so that all interested parties, including the research community, can examine and understand them. In particular, charging for access to standards, particularly during the development and public comment period, is incompatible with the transparency guarantee in NISTIR 7977.[2]

[1] ISO/IEC 19790:2012 Information technology – Security techniques – Security requirements for cryptographic modules http://www.iso.org/iso/catalogue_detail.htm?csnumber=52906

[2] NISTIR 7977 NIST Cryptographic Standards and Guidelines Development Process http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7977.pdf

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

If NIST believes that ISO 19790 is a crucial component of a revised FIPS-140, then NIST needs to find a way to make the standard publically available. The Board does not have a position on whether a token charge (for instance $1) would satisfy the requirement of public availability. The Board does feel strongly that NISTIR 7977 expresses the proper approach to cryptographic standards: that cryptographic standards should be completely open and that all interested parties should have access to essential information (which surely includes the text of the standard) throughout the development and lifetime of the standard. In this age of widespread discussion and interest in cryptography, the entire public is an interested party.

The Board welcomes further discussion on this topic.

Sincerely,

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