UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899-
OFFICE OF THE DIRECTOR

AUG 2 9 2016

Mr. Chris Boyer
Chair
Information Security and Privacy Advisory Board
100 Bureau Drive
Gaithersburg, MD 20899

Dear Mr. Boyer,

I would like to respond to the letter of April 20, 2016, from the Information Security and Privacy Advisory Board (ISPAB) Chair, regarding the update of Federal Information Processing Standards (FIPS) Publication140, "Security Requirements for Cryptographic Modules," with reference to an international standard.

The National Institute of Standards and Technology (NIST), and particularly the Computer Security Division (CSD), have consistently strived to engage NIST's primary cryptographic stakeholders within Federal agencies, voluntary standards developing organizations, and the research community. NIST appreciates the Board's expression of support for revision of FIPS 140, as well as its support for alignment of the FIPS with international standards.

This is in keeping with the statutory mandate that Federal agencies, in developing standards, "shall take into consideration international standards and shall, if appropriate, base the standards on international standards." 19 U.S.C. § 2532. And, as noted in Office of Management and Budget (OMB) Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities," the U.S. is obligated under the World Trade Organization (WTO) Agreement on Technical Barriers to Trade (TBT) "to use relevant international standards, except where such standards would be an ineffective or inappropriate means to fulfill the legitimate objective pursued."

NIST intends to recommend that the Secretary of Commerce approve ISO/IEC 19790:2012, Information technology – Security techniques – Security requirements for cryptographic modules, and ISO/IEC 24759:2014, Information technology – Security techniques – Test requirements for cryptographic modules, as U.S. government standards. One of the primary considerations in making this recommendation is to enable international collaboration on the testing processes and artifacts necessary to determine efficacy of the assurance case being made by the cryptographic implementation vendor and testing laboratory.

NIST

NIST understands the concern raised in the ISPAB's letter. Indeed, OMB Circular A-119 identifies the cost to regulated and other interested parties to access incorporated materials as one of several factors agencies should take into account in determining whether a standard is "reasonably available." Where material is copyrighted or otherwise subject to legal protection and not freely available, the Circular encourages agencies to work with the relevant standards developer to promote the availability of the materials, consistent with applicable law, such as through the use of technological solutions, low-cost-publication, or other appropriate means, while respecting the copyright owner's interest in protecting its intellectual property.

Accordingly, NIST CSD has been in discussions with the American National Standards Institute (ANSI)/InterNational Committee for Information Technology Standards (INCITS) to procure 2,000 perpetual copies of ISO/IEC 19790 and ISO/IEC 24759, so as to enable CSD to make these copies available to U.S. cryptography vendors, testing laboratories, researchers, academics, implementers, and government customers who might not otherwise have the means to obtain these references. CSD's discussions with ANSI/INCITS also address posting of these standards on a freely available web portal during the open comment period for the FIPS 140 revision.

The contributions of the ISPAB are valued by NIST as an independent feedback mechanism on our work in cryptography. I would like to thank the Board for its thoughtful leadership and efforts to help us make NIST a truly impactful and relevant agency.

Sincerely,

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