Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Docket No. 150706577-5577-01

RIN 0693-XC051

Government Use of Standards for Security and Conformance Requirements for Cryptographic Algorithm and Cryptographic Module Testing and Validation Programs.

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; Request for information.

SUMMARY: NIST is seeking public comment on the potential use of certain International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) standards for cryptographic algorithm and cryptographic module testing, conformance, and validation activities, currently specified by Federal Information Processing Standard (FIPS) 140-2. The National Technology Transfer and Advancement Act (NTTAA) directs federal agencies to adopt voluntary consensus standards wherever possible. The responses to this request for information will be used to plan possible changes to the FIPS or in a decision to

use all or part of the ISO/IEC standards for testing, conformance and validation of cryptographic algorithms and modules.

DATES: Comments on the potential use of ISO/IEC 19790:2014 must be received no later than 5 P.M, EST on [[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Written comments concerning the potential use of ISO/IEC 19790:2014 should be sent to: Information Technology Laboratory, ATTN Use of ISO/IEC 19790, Mail Stop 7730, National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, MD 20899.

Electronic comments should be sent to: UseOfISO@nist.gov.

FOR FURTHER INFORMATION CONTACT: Ms. Diane Honeycutt, telephone (301) 975-8443, MS 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899 or via e-mail at DHoneycutt@nist.gov.

SUPPLEMENTARY INFORMATION: The National Technology Transfer and Advancement Act (NTTAA), Pub. L. 104-113, directs federal agencies with respect to their use of and participation in the development of voluntary consensus standards. The NTTAA's

objective is for federal agencies to adopt voluntary consensus standards, wherever possible, in lieu of creating proprietary, non-consensus standards. As the implementation of commercial cryptography, which is used to protect U.S. non-national security information and information systems, is now commoditized and built, marketed and used globally, NIST is seeking comments on using the ISO/IEC 19790:2014 Security Requirements for Cryptographic Modules standard as the U.S. Federal Standard for cryptographic modules (http://www.iso.org/iso/catalogue_detail.htm?csnumber=59142).

The standards for cryptographic module testing, conformance, and validation activities are currently specified by Federal Information Processing Standard (FIPS) 140-2. This standard is used to ensure encryption technologies used by the U.S. Government meet minimally acceptable requirements and can demonstrate an acceptable level of conformance to the Standard that is commensurate with the risk the U.S. Government finds acceptable when using encryption technologies to protect U.S. Government information and information systems.

NIST is interested in the commercial and market effects to U.S. industry and the potential changes to visibility in cryptographic modules conformance to standards, as well as the ISO/IEC 19790:2014 standards ability to meet requirements for the U.S. Government. NIST is also interested in comments on the possible uses of ISO/IEC 19790:2014 that range from use of only selected sections, continuing with a FIPS requirement that cites a baseline version of the ISO/IEC 19790:2014, and/or full use of the ISO/IEC standard.
NIST is also interested in feedback on the impacts of a potential U.S. Government requirement for use and conformance using a standard with a fee-based model where organizations must purchase copies of the ISO/IEC 19790:2014.

NIST is particularly interested in comments from commercial implementers of cryptography, testing and conformance organizations, users of cryptography, and organizations who currently require or cite FIPS 140-2 as a normative reference, on the benefits versus risks in using ISO/IEC 19790:2014 rather than FIPS 140-2 from perspectives of technology, implementations, risks and impacts to commercial IT markets. NIST requests comments on the following questions regarding the use of ISO/IEC 19790:2014, but comments on other cryptographic test and conformance issues will also be considered.

1) Have your customers or users asked for either ISO/IEC 19790:2014 or FIPS 140-2 validations in cryptographic products?
2) Have the markets you serve asked for either validation and have you noticed any changes in what the markets you serve are asking for?
3) Do you think the ISO/IEC 19790:2014 standard specifies tests and provides evidence of conformance for cryptographic algorithms and modules better, equally or less as compared to FIPS 140-2 and in what areas?
4) Is there a difference in risk that you perceive would be mitigated or accepted in use of one standard versus the other?
5) Are the requirements in ISO/IEC 19790:2014 specific enough for your organization to develop a cryptographic module that can demonstrate conformance to this standard?
6) Would the U.S. Government citation of an ISO standard that has a fee for access to the standard inhibit your use or implementation of this standard?
7) Do either FIPS 140-2 or ISO/IEC 19790:2014 have a gap area that is not required for implementation, test or validation that presents an unacceptable risk to users of

cryptographic modules?

The responses to this request for information will be used to plan possible changes to the FIPS or in a decision to use all or part of ISO/IEC 19790:2014 for testing, conformance and validation of cryptographic algorithms and modules. In any decision made, it is the intention of NIST to continue specifying requirements for cryptography and cryptographic mechanisms used by the U.S. Government and a program for commercial products to demonstrate conformance to those requirements. It is also the intention of NIST to continue to specify the cryptographic modules, modes and key management schemes that are acceptable for use by the U.S. Government to protect its information and information systems regardless of any test, conformance or validation standards decision.

Authority:

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce, pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Pub. L. 104-106), and the Federal Information Security Management Act of 2002 (Pub. L. 107-347).

Kevin Kimball
Chief of Staff
[FR Doc. 2015-19743 Filed: 8/11/2015 08:45 am; Publication Date: 8/12/2015]