Billing Code 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 170810743-8858-01]

RIN 0693-XC079

Announcing Issuance of Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules

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

ACTION: Notice.

SUMMARY: This notice announces the Secretary of Commerce's issuance of Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules. FIPS 140-3 includes references to existing International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19790:2012(E) *Information technology — Security techniques — Security requirements for cryptographic modules* and ISO/IEC 24759:2017(E) *Information technology — Security techniques — Test requirements for cryptographic modules*. As permitted by the standards, the NIST Special Publication (SP) series 800-140 will specify updates, replacements, or additions to the currently cited ISO/IEC standard as necessary.

DATES: FIPS 140-3 is effective September 22, 2019. FIPS 140-3 testing will begin on September 22, 2020. FIPS 140-2 testing will continue for at least a year after FIPS 140-3 testing begins.

ADDRESSES: FIPS 140-3 is available electronically from the NIST web site at: *https://csrc.nist.gov/publications/fips*. Comments that were received on the proposed changes are also published electronically at *https://csrc.nist.gov/projects/fips-140-3-development*.

FOR FURTHER INFORMATION CONTACT: Michael Cooper, (301) 975–8077, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: *michael.cooper@nist.gov*.

SUPPLEMENTARY INFORMATION: NIST has been participating in the ISO/IEC process for developing standards for cryptographic modules and working closely with international industry to unify several cryptographic security standards. ISO/IEC 19790:2012(E), *Information technology — Security techniques — Security requirements for cryptographic modules*, is an international standard based on updates of the earlier versions of FIPS 140, *Security Requirements for Cryptographic Modules*. ISO/IEC 24759:2017(E), *Information technology — Security techniques — Test requirements for cryptographic modules* is an international standard based on the Derived Test Requirements for FIPS 140-2, *Security Requirements for Cryptographic Modules*. The National Technology Transfer and Advancement Act (NTTAA), Public Law 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. 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. Therefore, FIPS 140-3 applies ISO/IEC 19790:2012(E) and ISO/IEC 24759:2017(E) as the security requirements for cryptographic modules. The SP 800-140 series, which is currently under development, will be used to specify updates, replacements, or additions to requirements as allowed

by ISO/IEC 19790:2012(E), with the Cryptographic Module Validation Program (CMVP) executing the role of the validation authority as defined in the ISO/IEC standard.[1] During the transition period prior to FIPS 140-3 becoming effective, FIPS 140-2 testing will continue, and NIST will introduce the SP 800-140 series documents (at *https://csrc.nist.gov/publications/sp800*). The series is expected to consist of:

- SP 800-140, *FIPS 140-3 Derived Test Requirements (DTR);*
- SP 800-140A, *CMVP Documentation Requirements;*
- SP 800-140B, *CMVP Security Policy Requirements;*
- SP 800-140C, *CMVP Approved Security Functions;*
- SP 800-140D, *CMVP Approved Sensitive Security Parameter Generation and Establishment Methods;*
- SP 800-140E, *CMVP Approved Authentication Mechanisms;* and
- SP 800-140F, *CMVP Non-Invasive Attack Mitigation Test Metrics.*

FIPS 140-1, first published in 1994, was developed by a government and industry working group. The working group identified requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million-dollar funds transfers, and life protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Four security levels were specified for each of 11 requirement areas. Each security level offered an

[1] ISO/IEC 19790 defines the validation authority as the entity that will validate the test results for conformance to this international standard.

increase in security over the preceding level. These four increasing levels of security allowed cost-effective solutions that were appropriate for different degrees of data sensitivity and different application environments.

In 2001, FIPS 140-2 superseded FIPS 140-1. FIPS 140-2 incorporated changes in applicable standards and technology since the development of FIPS 140-1 as well as changes that were based on comments received from the public. Though the standard was reviewed after five years, consensus to move forward was not achieved until the 2012 revision of ISO/IEC 19790.

FIPS 140-3 supercedes FIPS 140-2. FIPS 140-3 aligns with ISO/IEC 19790:2012(E) with modifications of the Annexes allowed by the specific user communities. The testing for these requirements shall be in accordance with ISO/IEC 24759:2017(E), with the modifications, additions or deletions of vendor evidence and testing allowed as a validation authority under paragraph 5.2 of ISO/IEC 24759:2017(E).

On August 12, 2015, NIST published a notice in the Federal Register (80 FR 48295) requesting public comments on the potential use of ISO/IEC standards for cryptographic algorithm and cryptographic module testing, conformance, and validation activities, currently specified by FIPS 140-2. Comments were submitted by 17 entities, including four accredited cryptographic testing laboratories, eight vendors of cryptographic modules, one industry association, and four individuals. Some comments only addressed specific aspects of the proposal. Eleven of the comments supported a revised standard, five were neutral and one was opposed. Many comments asked for clarification on the continued use of implementation guidance and administration guidance to the testing laboratories. NIST will consolidate the implementation guidance and administration guidance into the SP 800-140 series documents, which will be made available for public review and comment. Other comments provided feedback on

perceived market demand, comparisons of test coverage between FIPS 140-2 and the ISO/IEC standards and the potential risks that might be assumed with the use of the ISO/IEC standard. Most of the commenters were concerned about the payment model for accessing and obtaining the ISO/IEC standards compared with the free access to the current FIPS 140-2. All of the suggestions, questions, and recommendations within the scope of NIST's request for comments were carefully reviewed, and changes were made to the FIPS, where appropriate. Some comments submitted questions or raised issues that were related but outside the scope of this FIPS. Comments that were outside the scope of this FIPS, but that were within the scope of one of the related Special Publications, are deferred for later consideration in the context of development of the SP 800-140 series.

The following is a summary and analysis of the comments received during the public comment period, and NIST's responses to them, including the interests, concerns, recommendations, and issues considered in the development of FIPS 140-3:

Comment: Nine commenters responded that they have been asked by customers about testing for ISO/IEC standards or have had requests to test using the ISO/IEC standard.

Response: NIST will be revising its guidance by moving to the ISO/IEC standards embraced in FIPS 140-3.

Comment: Seven commenters responded that they were concerned about the ability of researchers, academics and small organizations to obtain the ISO/IEC standard due to the payment model used by ISO/IEC.

Response: NIST intends to work with the appropriate parties to help ensure that the ISO/IEC standard will be made reasonably available to researchers, academics and small organizations.

Comment: Eleven commenters indicated that changing to the ISO/IEC standard did not increase the risk of using cryptography or decrease trust in the use of cryptography as compared to the current FIPS 140-2.

Response: NIST intends to make the normative reference to the ISO/IEC standard specific to a version that NIST believes is acceptable to provide assurances in the cryptography used by the Federal Government. In its role as the approval authority[2] under ISO/IEC 19790:2012(E), NIST is permitted to replace most of the supporting requirements with NIST guidance, most of which are currently utilized in the existing FIPS 140-2.

Comment: One commenter expressed concern that adoption of an international, consensus based standard would put the US in the position of using future versions of the ISO/IEC standard as it is updated and evolves.

Response: NIST plans on continuing its robust participation in the relevant ISO/IEC working groups, and will thoroughly discuss any changes necessary to keep these requirements relevant. If an update or change is made to the ISO/IEC standards that NIST does not feel is adequate for the security needs of the Federal Government, NIST will have the flexibility to adopt a different standard. By working with ISO/IEC experts, NIST can maintain flexibility within the standards as allowed by the validation authorities as described in the ISO/IEC standards. Should these measures prove insufficient, NIST can, through FIPS 140-3 or the SP 800-140 series development process, create a revised standard, controlled by NIST, to maintain the most secure posture possible.

[2] ISO/IEC 19790 defines the approval authority as any national or international organization/authority mandated to approve and/or evaluate security functions.

FIPS 140-3 is available electronically from the NIST web site at:

https://csrc.nist.gov/publications/fips.

Authority: 44 U.S.C. 3553(f)(1), 15 U.S.C. 278g-3.

Kevin A. Kimball,

Chief of Staff.

[FR Doc. 2019-08817 Filed: 4/30/2019 8:45 am; Publication Date: 5/1/2019]