Billing Code: 3510-13

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 110107015-1402-02]

Announcing Approval of Federal Information Processing Standard (FIPS) Publication 180-4, Secure Hash Standard (SHS); a revision of FIPS 180-3.

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

ACTION: Notice.

SUMMARY: This notice announces the Secretary of Commerce's approval of Federal Information Processing Standard (FIPS) Publication 180-4, Secure Hash Standard (SHS). FIPS 180-4 updates FIPS 180-3 by providing a general procedure for creating an initialization value, adding two additional secure hash algorithms to the Standard: SHA-512/224 and SHA-512/256 and removing a restriction that padding must be done before hash computation begins, which was required in FIPS 180-3.

DATES: The approved Standard is effective as of [please insert date of publication of this notice in the Federal Register].

FOR FURTHER INFORMATION CONTACT: Elaine Barker, (301) 975–2911, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899–8930, email: elaine.barker@nist.gov, or Quynh Dang, (301) 975-3610, email: quynh.dang@nist.gov.

SUPPLEMENTAL INFORMATION:

This notice announces the Secretary of Commerce's approval of Federal Information Processing Standard (FIPS) Publication 180-4, Secure Hash Standard (SHS). FIPS 180-4 updates FIPS 180-3 by providing a general procedure for creating an initialization value, adding two additional secure hash algorithms to the Standard: SHA-512/224 and SHA-512/256, and removing a restriction that padding must be done before hash computation begins, which was required in FIPS 180-3. SHA-512/224 and SHA-512/256 may be more efficient alternatives to SHA-224 and SHA-256 respectively, on platforms that are optimized for 64-bit operations. Removing the restriction on the padding operation in the secure hash algorithms will potentially allow more flexibility and efficiency in implementing the secure hash algorithms in many computer network applications.

On February 11, 2011, NIST published a notice in the Federal Register (76 FR 7817) announcing the availability of draft FIPS 180–4, and soliciting comments on the draft standard from the public, research communities, manufacturers, voluntary standards organizations and Federal, State and local government organizations. Comments were received from two corporations and one individual. The following is a summary of the specific comments and NIST's responses to them:

Comment: One commenter requested NIST to provide more detail for the calculation of the initialization values for SHA-512/224 and SHA-512/256, especially for the variable *t*.

Response: Clarification of the variable "t" has been provided in the FIPS. Sufficient examples are provided at the website: http://csrc.nist.gov/groups/ST/toolkit/examples.html, as indicated in the APPENDIX A of the FIPS.

Comment: One commenter indicated that the notation for SHA-512("SHA-512/t") and SHA-512("SHA-512/256") needs to be further defined, including a definition for ASCII strings.

Response: Clarification of the variable "*t*" was provided in Section 5.3.6 of the FIPS, along with further clarification of the input string to the SHA-512 hash function.

Comment: One commenter requested NIST to define SHA-512/160 as an approved hash algorithm.

Response: NIST believes that there is not much demand for a new SHA-512-based hash algorithm with 160-bit hash output at this time, since generating digital signatures using 160-bit hash values will be not approved after the year 2013.

FIPS 180-4 is available electronically from the NIST web site at: http://csrc.nist.gov/publications/PubsFIPS.html.

AUTHORITY: In accordance with the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347), the Secretary of Commerce is authorized to approve Federal Information Processing Standards (FIPS). NIST activities to develop computer security standards to protect Federal sensitive (unclassified) information systems are undertaken pursuant to specific responsibilities assigned to NIST by section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended by section 303 of the Federal Information Security Management Act of 2002.

Dated: March 1, 2012

Willie E. May
Associate Director for Laboratory Programs

[FR Doc. 2012-5400 Filed 03/05/2012 at 8:45 am; Publication Date: 03/06/2012]