Dated: July 23, 2008.

David M. Spooner,

Assistant Secretary for Import Administration.

[FR Doc. E8–17365 Filed 7–28–08; 8:45 am]

BILLING CODE 3510–DS–S

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 070413089–8493–02]

Announcing Approval of Federal Information Processing Standard (FIPS) Publication 198–1, The Keyed-Hash Message Authentication Code (HMAC), a Revision of FIPS 198

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

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) announces approval of Federal Information Processing Standard (FIPS) Publication 198–1, The Keyed-Hash Message Authentication Code (HMAC), a revision of FIPS 198. The FIPS specifies a mechanism for message authentication using cryptographic hash functions in federal information systems. The technical information about the security provided by the HMAC algorithm, and the length limit and security implications of truncated HMAC outputs have been removed from the revised standard. This information may need frequent updating, and its removal from the specification will enable NIST to employ a more effective process for keeping the information current. NIST will provide specific guidelines about the security provided by the HMAC and the use of truncation techniques for it in Special Publication (SP) 800–17, which can be updated in a timely manner as the technical conditions change.

DATES: The approval changes are effective as of July 29, 2008.

FOR FURTHER INFORMATION CONTACT: Elaine Barker, Telephone (301)975–2911, or via e-mail at *elaine.barker@nist.gov* or Quynh Dang, (301) 975–3610, e-mail: *quynh.dang@nist.gov*, National Institute of Standards and Technology, 100 Bureau Drive, Mailstop 8930, Gaithersburg, MD 20899. FIPS 198–1 is available electronically from the NIST Web site at: *http://csrc.nist.gov/publications/PubsFIPS.html*. NIST Special Publications (SPs) are available electronically from the NIST Web site at: *http://csrc.nist.gov/publications/PubsFIPS.html*.

SUPPLEMENTARY INFORMATION: On June 12, 2007, NIST published a notice in the **Federal Register** (72 FR 32281), announcing draft FIPS 198–1, and soliciting comments on draft standard from the public, research communities, manufacturers, voluntary standards organizations and federal, state and local government organizations. In addition, to being published in the **Federal Register**, the notice was posted on the NIST web pages. Information was provided about the submission of electronic comments and an electronic template for the submission of comments was made available.

NIST received comments, responses, and questions from three federal government organizations and two from the public. The comments received asked for clarification of the text of the standard or recommended editorial and formatting changes. None of the comments opposed the approval of the revised standard. All of the suggestions and recommendations were carefully reviewed, and changes were made to the standard where appropriate. The following is the summary of the specific comments and NIST's responses to them:

Comment: What are the changes between FIPS 198 and FIPS 198–1?

Response: The length specifications for the truncated HMAC outputs and their security implications are no longer discussed in this Standard; instead, they are included in SP 800–107. The discussion about the limitations of MAC algorithms has been moved to SP 800–107. Examples and OIDs have been removed from the standards and are now posted on a NIST Web site that is identified in the Standard. This list of changes has been provided in Appendix A.

Comment: ''K'' in the last sentence of Section 3 should be changed ''K0'' to be consistent with Section 4.

Response: NIST revised the text in Section 3 to improve the clarity of the meaning of the text.

Comment: The first paragraph of Section 5 talks about replacing one of the hashes with a different hash. The need for this paragraph is not clearly understood.

Response: NIST revised Section 5 to improve the clarity of the intended meaning of the text.

Comment: Why has truncation been removed from the algorithm specification?

Response: Truncation is still addressed in FIPS 198–1. However, the length of the truncated HMAC outputs and the security implications of truncation are not discussed in this Standard; instead, they are discussed in SP 800–107. A pointer to SP 800–107 has been provided in FIPS 198–1.

Comment: Why is the security of the HMAC not mentioned in the FIPS 198–1?

Response: The discussion on the limitations of the MAC algorithms (*i.e.*, the security discussion) has been moved to SP 800–107. A pointer to SP 800–107 has been provided in FIPS 198–1.

Comment: A number of editorial and legal text changes were suggested.

Response: NIST made the suggested changes.

Comment: Change 0x00 to x‘00’ in Step 3 of Table 1 to make it consistent with the definition in Section 2.3.

Response: NIST made the suggested change.

Comment: Figure 1 does not accurately represent the steps in the HMAC algorithm.

Response: NIST reviewed Figure 1 and determined that it is accurate.

Security issues related to the HMAC algorithm, its applications and truncation limitations are addressed in draft NIST Special Publication 800–107, Recommendation for Using Approved Hash Algorithms. Draft NIST Special Publication 800–107 will become NIST Special Publication 800–107 in the near future.

Authority: In accordance with the Information Technology Management Reform Act of 1996 (Pub. L. 104–106) and the Federal Information Security Management Act (FISMA) of 2002 (Pub. L. 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 (5 U.S.C. 278g–3) as amended by section 303 of the Federal Information Security Management Act of 2002.

E.O. 12866: This notice has been determined not be significant for the purpose of E.O.12866.

Dated: July 21, 2008.

James M. Turner,

Deputy Director.

[FR Doc. E8–17363 Filed 7–28–08; 8:45 am]

BILLING CODE 3510–13–P