This Order is effective upon date of publication in the **Federal Register** and shall remain in effect for 180 days.

Entered this 1st day of June, 2007.

Darryl W. Jackson,

Assistant Secretary of Commerce for Export Enforcement.

[FR Doc. 07–2899 Filed 6–11–07; 8:45 am]

BILLING CODE 3510–DT–M

DEPARTMENT OF COMMERCE

International Trade Administration

[A–570–890]

Wooden Bedroom Furniture from the People's Republic of China: Extension of Time Limits for the Final Results of the Antidumping Duty Administrative Review and New Shipper Reviews

AGENCY: Import Administration, International Trade Administration, Department of Commerce.

EFFECTIVE DATE: June 12, 2007.

FOR FURTHER INFORMATION CONTACT: Gene Degnan, AD/CVD Operations, Office 8, Import Administration, International Trade Administration, U.S. Department of Commerce, 14th Street and Constitution Avenue, NW, Washington, DC 20230; telephone: (202) 482–0414.

SUPPLEMENTARY INFORMATION:

Background

The Department of Commerce (''the Department'') published an antidumping duty order on wooden bedroom furniture (''WBF'') from the People's Republic of China (''PRC'') on January 4, 2005. *See Notice of Amended Final Determination of Sales at Less Than Fair Value and Antidumping Duty Order: Wooden Bedroom Furniture From the People's Republic of China*, 70 FR 329 (January 4, 2005). On March 7, 2006, the Department published in the **Federal Register** a notice of the initiation of the antidumping duty administrative review of WBF from the PRC and new shipper reviews for the period June 24, 2004, through December 31, 2005. *See Initiation of Administrative Review of Antidumping Duty Order on Wooden Bedroom Furniture from the People's Republic of China*, 71 FR 11394 (March 7, 2006) and *Wooden Bedroom Furniture from the People's Republic of China: Initiation of New Shipper Reviews*, 71 FR 11404 (March 7, 2006) (''*Initiation of Second Annual New Shipper Reviews*''). On August 24, 2006, the Department aligned the deadlines and the time limits of the new shipper reviews of WBF with the 2004–2005 administrative review of WBF. *See* Memorandum to the File from Lilit Astvatsatrian, Case Analyst, through Wendy Frankel, Office Director, dated August 24, 2006. On February 9, 2007, the Department published in the **Federal Register** the preliminary results of the first administrative review and the new shipper reviews. *See Wooden Bedroom Furniture from the People's Republic of China: Preliminary Results of Antidumping Duty Administrative Review, Preliminary Results of New Shipper Reviews and Notice of Partial Rescission*, 72 FR 6201 (February 9, 2007). The final results of review are currently due no later than June 9, 2007.

Extension of Time Limit of Final Results

Section 751(a)(3)(A) of the Tariff Act of 1930, as amended (''the Act''), requires the Department to issue final results within 120 days after the date on which the preliminary results are published. However, if it is not practicable to complete the review within this time period, section 751(a)(3)(A) of the Act allows the Department to extend the time period to a maximum of 180 days. Completion of the final results of the administrative review within the 120-day period is not practicable because the Department conducted verification in the administrative review after publication of the preliminary results, and, therefore, needs additional time to complete post–preliminary results verification reports, invite and analyze comments by interested parties on the preliminary results and verification reports, and analyze information gathered at verification.

Because it is not practicable to complete this review within the time specified under the Act, we are extending the time period for issuing the final results of the administrative and new shipper reviews to 180 days, until August 8, 2007, in accordance with section 751(a)(3)(A) of the Act. This notice is published pursuant to sections 751(a) and 777(i) of the Act.

Dated: June 5, 2007.

Stephen J. Claeys,

Deputy Assistant Secretaryfor Import Administration.

[FR Doc. E7–11318 Filed 6–11–07; 8:45 am]

BILLING CODE 3510–DS–S

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 070413089–7091–01]

Announcing Draft Federal Information Processing Standard (FIPS) Publication 198–1, the Keyed-Hash Message Authentication Code, and Request for Comments

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice and request for comments.

SUMMARY: This notice announces the Draft Federal Information Processing Standard (FIPS) 198–1, the Keyed-Hash Message Authentication Code (HMAC), for public review and comment. The draft standard, designated ''Draft FIPS 198–1,'' is proposed to supersede FIPS 198, the Keyed-Hash Message Authentication Code, issued March 2002. FIPS 198–1 specifies a keyed-hash message authentication code (HMAC), a mechanism for message authentication using cryptographic hash functions and shared secret keys. The proposed standard is available at *http://csrc.nist.gov/publications/drafts.html.*

Prior to the submission of this proposed standard to the Secretary of Commerce for review and approval, it is essential that consideration be given to the needs and views of the public, users, the information technology industry, and Federal, State, and local government organizations. The purpose of this notice is to solicit such views.

DATES: Comments must be received by September 10, 2007.

ADDRESSES: Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, Attention: Comments on Draft FIPS 198–1, 100 Bureau Drive—Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930. Electronic comments may be sent to *proposed198–1@nist.gov.* with a subject line of Keyed-Hash Message Authentication Code. The current FIPS 198 and its proposed replacement, Draft FIPS 198–1, are available electronically at *http://csrc.nist.gov/publications/index.html.*

Comments received in response to this notice will be published electronically at *http://csrc.nist.gov/CryptoToolkit/tkhash.html.*

FOR FURTHER INFORMATION CONTACT: For general information, contact: Elaine Barker, National Institute of Standards and Technology, Stop 8930,

Gaithersburg, MD 20899–8930, telephone: 301–975–2911 or via fax at 301–975–8670, e-mail: *elaine.barker@nist.gov.* or Quynh Dang, telephone: 301–975–3610, e-mail: *quynh.dang@nist.gov.*

SUPPLEMENTARY INFORMATION: The changes between FIPS 198 and FIPS 198–1 are minor and are motivated by a desire to put informative information that may change in a separate, less formal publication that can be readily updated as necessary. FIPS 198 contained statements about the security provided by the HMAC algorithm and specified a truncation technique for the HMAC output. Since the security provided by the HMAC algorithm and its applications might be altered by future cryptanalysis, the security statements were not included in FIPS 198–1. The security of HMAC will be addressed in NIST Special Publications (SP) 800–57, Recommendation for Key Management, and 800–107, Recommendation for Using Approved Hash Algorithms. Draft FIPS 198–1 also does not include the truncation technique; the truncation technique of HMAC will be specified in the NIST Special Publication 800–107. Draft NIST Special Publications and NIST Special Publications are available at *http://csrc.nist.gov/publications/index.html.* Examples of the implementation of the HMAC algorithm can be found at *http://www.nist.gov/CryptoToolkitExamples.* NIST will continue to review these examples and to update them as needed.

Authority: NIST activities to develop computer security standards to protect Federal sensitive (unclassified) systems are undertaken pursuant to specific responsibilities assigned to NIST to 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 (Pub. L. 107–347). This notice has been determined not to be significant for the purposes of Executive Order 12866.

Dated: June 5, 2007.

James M. Turner,

Deputy Director, NIST.

[FR Doc. E7–11309 Filed 6–11–07; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 070413090–7092–01]

Announcing Draft Federal Information Processing Standard (FIPS) Publication 180–3, the Secure Hash Standard, and Request for Comments

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice and request for comments.

SUMMARY: This notice announces the Draft Federal Information Processing Standard (FIPS) 180–3, Secure Hash Standard (SHS), for public review and comment. The draft standard, designated ''Draft FIPS 180–3,'' is proposed to supersede FIPS 180–2. FIPS 180–2, Secure Hash Standard (SHS), August 2002, specifies secure hash algorithms (SHA) called SHA–1, SHA–256, SHA–384 and SHA–512. These algorithms produce 160, 256, 384, and 512-bit outputs, respectively, which are called message digests. An additional secure hash algorithm, called SHA–224, that produces a 224-bit output, is specified in Change Notice 1 to FIPS 180–2, which was issued in 2004. Draft FIPS 180–3 specifies five secure hash algorithms: SHA–1, SHA–224, SHA–256, SHA–384, and SHA–512. The proposed standard is available at *http://csrc.nist.gov/publications/drafts.html*.

Prior to the submission of this proposed standard to the Secretary of Commerce for review and approval, it is essential that consideration be given to the needs and views of the public, users, the information technology industry, and Federal, State, and local government organizations. The purpose of this notice is to solicit such views.

DATES: Comments must be received by September 10, 2007.

ADDRESSES: Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, Attention: Comments on Draft FIPS 180–3, 100 Bureau Drive—Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930. Electronic comments may be sent to: *Proposed180–3@nist.gov*. The current FIPS 180–2 and its proposed replacement, Draft FIPS 180–3, are available electronically at *http://csrc.nist.gov/publications/index.html*.

Comments received in response to this notice will be published electronically at *http://csrc.nist.gov/CryptoToolkit/tkhash.html*.

FOR FURTHER INFORMATION CONTACT: For general information, contact: Elaine Barker, National Institute of Standards and Technology, Stop 8930, Gaithersburg, MD 20899–8930, telephone: 301–975–2911, e-mail: *elaine.barker@nist.gov*. or via fax at 301–975–8670, or Quynh Dang, telephone: 301–975–3610, e-mail: *quynh.dang@nist.gov*.

SUPPLEMENTARY INFORMATION: The changes between FIPS 180–2 and FIPS 180–3 are minor and are motivated by a desire to put informative information that is subject to change in a less formal publication that can be readily updated as necessary. FIPS 180–2 contained statements about the security strengths of the hash algorithms. However, the security strengths of the hashing algorithms, SHA–1, SHA–224, SHA–256, SHA–384 and SHA–512, might change due to future cryptanalysis; consequently, Draft FIPS 180–3 does not describe their security strengths. Instead, the security strengths will be specified in NIST Special Publications (SP) 800–57, Recommendation for Key Management, and discussed in NIST SP 800–107, Recommendation for Using Approved Hash Algorithms. These Special Publications will be periodically reviewed and updated if warranted by advances in the cryptanalysis of these hash algorithms. Examples of the implementation of these hash algorithms can be found at *http://www.nist.gov/CryptoToolkitExamples*. NIST Special Publications are available at: *http://csrc.nist.gov/publications/index.html*.

Authority: NIST activities to develop computer security standards to protect Federal sensitive (unclassified) 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 (Pub. L. 107–347). Executive Order 12866: This notice has been determined not to be significant for the purpose of Executive Order 12866.

Dated: June 5, 2007.

James M. Turner,

Deputy Director, NIST.

[FR Doc. E7–11326 Filed 6–11–07; 8:45 am]

BILLING CODE 3510–13–P