review, in whole or in part, if a party that requested a review withdraws the request within 90 days of the date of publication of notice of initiation of the requested review. The Secretary may extend this time limit if the Secretary decides that it is reasonable to do so. *See* 19 CFR 351.213(d)(1). Both Petitioner and Akzo Nobel withdrew their requests for review with respect to the latter within the 90-day time limit. Therefore, in response to the withdrawal of requests for administrative reviews by both Akzo Nobel and Petitioner, the Department hereby rescinds the administrative review of the antidumping duty order on purified CMC from the Netherlands for the period July 1, 2007, through June 30, 2008 for Akzo Nobel.

Assessment Rates

The Department intends to issue assessment instructions to the U.S. Customs and Border Protection (''CBP'') 15 days after the date of publication of this partial rescission of administrative review. The Department will direct CBP to assess antidumping duties for Akzo Nobel at the cash deposit rate in effect on the date of entry for entries during the period July 1, 2007, through June 30, 2008.

Notification to Importers

This notice serves as a final reminder to importers for whom this review is being rescinded, of their responsibility under 19 CFR 351.402(f) to file a certificate regarding reimbursement of antidumping duties prior to liquidation of the relevant entries during this review period. Failure to comply with this requirement could result in the Secretary's presumption that reimbursement of antidumping duties occurred and the subsequent assessment of double antidumping duties.

Notification Regarding Administrative Protective Orders

This notice serves as a reminder to parties subject to administrative protective order (''APO'') of their responsibility concerning the disposition of proprietary information disclosed under APO in accordance with 19 CFR 351.305(a)(3). Timely written notification of the return or destruction of APO materials or conversion to judicial protective order is hereby requested. Failure to comply with the regulations and terms of an APO is a sanctionable violation.

This notice is published in accordance with sections 751(a)(1) and 777(i)(1) of the Tariff Act of 1930, as amended, and 19 CFR 351.213(d)(4).

Dated: November 4, 2008.

Stephen J. Claeys,

Deputy Assistant Secretary for Import Administration.

[FR Doc. E8–26836 Filed 11–10–08; 8:45 am]

BILLING CODE 3510–DS–S

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. [0810011295–81297–01]]

Announcing DRAFT Federal Information Processing Standard (FIPS) Publication 186–3, Digital Signature Standard (DSS) and Request for Comments

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

ACTION: Notice.

SUMMARY: This notice announces a second public review and comment period for Draft Federal Information Processing Standard 186–3, Digital Signature Standard. The draft standard, designated ''Draft FIPS 186–3,'' is proposed to revise and supersede FIPS 186–2. Draft FIPS 186–3 is a revision of FIPS 186–2, the Digital Signature Standard. The Draft FIPS specifies three techniques for the generation and verification of digital signatures that can be used for the protection of data: the Digital Signature Algorithm (DSA), the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Rivest-Shamir-Adelman (RSA) algorithm. Although all three of these algorithms were approved in FIPS 186–2, this revision increases the key sizes allowed for DSA, provides additional requirements for the use of RSA and ECDSA, and includes requirements for obtaining the assurances necessary for valid digital signatures. FIPS 186–2 contained specifications for random number generators (RNGs); this revision does not include such specifications, but refers to NIST Special Publication (SP) 800–90 for obtaining random numbers.

Prior to the submission of this proposed standard to the Secretary of Commerce for review and approval, it is essential that consideration is 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 on or before December 12, 2008.

ADDRESSES: Written comments may be sent to: Chief, Computer Security Division, Information Technology Laboratory, Attention: Comments on Draft FIPS 186–3, 100 Bureau Drive—Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930. Electronic comments may also be sent to: *ebarker@nist.gov.*

FOR FURTHER INFORMATION CONTACT: Elaine Barker, (301) 975–2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930, *e-mail: elaine.barker@nist.gov.*

SUPPLEMENTARY INFORMATION: FIPS 186, first published in 1994, specified a digital signature algorithm (DSA) to generate and verify digital signatures. Later revisions (FIPS 186–1 and FIPS 186–2, adopted in 1998 and 1999, respectively) adopted two additional algorithms specified in American National Standards (ANS) X9.31 (Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)), and X9.62 (The Elliptic Curve Digital Signature Algorithm (ECDSA)).

The original DSA algorithm, as specified in FIPS 186, 186–1 and 186–2, allows key sizes of 512 to 1024 bits. With advances in technology, it is prudent to consider larger key sizes. Draft FIPS 186–3 allows the use of 1024, 2048 and 3072-bit keys. Other requirements have also been added concerning the use of ANS X9.31 and ANS X9.62. In addition, the use of the RSA algorithm as specified in Public Key Cryptography Standard (PKCS) #1 (RSA Cryptography Standard) is allowed.

A request for public comments was published in the **Federal Register** on March 13, 2006 (71 FR 12678). After receiving comments in response to this notice, NIST incorporated the comments and posted a revised version of the FIPS on its Web site. NIST received some additional comments in response to this posting. In all, a total of 15 individuals and organizations provided comments (two U.S. government agencies, a foreign government agency, one university, eight private organizations, and three from individuals). The following is a summary of the comments received and NIST's responses to them:

Comment: Seven commenters suggested a number of editorial changes.

Response: NIST made the appropriate editorial changes, which included correcting typographical errors; spelling, format and font size changes; reference restrictions and updates, where appropriate; minor word changes and clarifications.

Comment: One commenter requested that examples be provided for each of the digital signatures algorithms and key sizes.

Response: Examples will be provided at *http://csrc.nist.gov/groups/ST/toolkit/examples.html*, and a link to this Web page has been included in the implementation section of the announcement.

Comment: Eight commenters suggested a number of minor technical changes.

Response: The appropriate changes were made, which included:

Corrections to the input to and pseudocode for defined functions;

Corrections to table entries;

Removal of the appendix on timestamping, and placing the contents in a different document;

Allowing the use of the Chinese Remainder Theorem (CRT) for the representation of the private key; and

Stating that the minimum lengths for the auxiliary primes for the generation of RSA keys may be either fixed or randomly chosen.

Comment: Two commenters noted that the allowed values for the public exponent e differ significantly from those allowed in ANS X9.31 and PKCS #1.

Response: The restricted values in the FIPS are a Federal government choice to provide a higher level of security for its agencies. Non-Federal government entities may voluntarily adopt these restrictions.

Comment: One commenter asked why the new DSA domain parameter validation method in A.1.1.3 is not compatible with the old verification method in A.1.1.1, since the change breaks interoperability with the FIPS 186–2 generation method.

Response: A.1.1.3 is intentionally different from A.1.1.1. The change in the use of the hash function (no XORing) was in response to a cryptanalytic attack that showed how to select a set of domain parameters generated in the A.1.1.1 fashion in such a way that two ''messages'' with the same DSA signature could be found. Note that A.1.1.1 still allows domain parameters generated using the older method to be verified.

Comment: One commenter asked why the DSA key sizes are limited to the smaller values?

Response: The length of the larger keys has a huge impact on communications and storage requirements. The strategy of the U.S. government is to transition to elliptic curve algorithms in order to reduce the key sizes.

Comment: One commenter asked that a specification of the Shawe-Taylor algorithm be included for use in the generation of RSA primes, as well as for DSA primes.

Response: The Shawe-Taylor method was rewritten as a general routine that is used for both DSA and RSA prime generation.

Comment: Two commenters provided comments with regard to the inconsistencies in the number of iterations required for the probabilistic primality tests.

Response: The number of iterations was taken from several FIPS and ANSI standards. As a result of these comments, NIST reviewed the methods used to calculate the number of iterations and calculated new values for each digital signature method and prime length.

After the proposed values and associated explanatory text were posted on the NIST Web site (in January 2007) the following five comments were received:

Comment: One commenter stated the values in ANS X9.80 (Prime Number Generation, Primality Testing, and Primality Certificates) should be used for the number of iterations.

Response: The values ANS X9.80 were based on assumptions and estimates that have been superseded by more recent considerations, and these newer values have been included the FIPS.

Comment: One commenter suggested that fewer categories be provided in the tables.

Response: NIST has chosen to base the number of tests on the key sizes and provided separate requirements for each. An implementer can choose to combine the requirements into fewer categories, as long as the number of rounds for each key size are equal to or greater than the numbers provided in the FIPS.

Comment: One commenter felt that the error probability should always be 2^{-100} to align with the ANSI standards.

Response: The 2^{-100} error probability is included in FIPS 186–3, along with others that are dependent on the security strength, to allow an implementer to select the most suitable probability for their application.

Comment: One commenter asked why the Lucas test is not required in some cases?

Response: After extensive analysis by NIST, it was determined the Lucas test is not required. However, the test can be performed after the required number of iterations of the Miller-Rabin tests in order to provide higher assurance. Wording has been included to clarify this.

Comment: One commenter suggested that the Frobenius-Grantham (FG) method for prime candidate testing should be included, in addition to the Miller-Rabin (MR) and Lucas tests.

Response: NIST has decided to remain with the testing methods used in ANS X9.31, which includes the MR and Lucas tests, but not the FG tests. In addition, the FG tests are more complex, so would be more likely to be implemented incorrectly.

Comment: The criteria for the generation of strong primes in ASC X9.31, upon which RSA key generation is based, does not agree with the definition of strong primes in the Handbook of Applied Cryptography (HAC).

Response: NIST researched and analyzed the requirements for RSA key pair generation, including requirements for the use of strong primes, and determined that strong primes as defined by the HAC are not required. The RSA key pair generation methods were modified to include a number of different methods that were not previously included in the draft FIPS.

Comment: The draft FIPS refers to approved random number generators. It is not clear whether SP 800–90 contains the only approved methods for random number generation, or if other approved methods can be used.

Response: The only other NIST document containing approved methods for random number generation is FIPS 186–2. With the approval of FIPS 186–3, those methods will no longer be approved, subject to a transition period posted by the Cryptographic Module Validation Program (CMVP).

NIST has incorporated the comments previously received as described above. NIST now seeks public comments on the revised draft of FIPS 186–3. This second draft of FIPS 186–3 is available electronically from the NIST Web site at: *http://csrc.nist.gov/publications/drafts.html.* The current FIPS 186–2 is available electronically from the NIST Web site at: *http://csrc.nist.gov/publications/fips/index.html.* The first draft of FIPS 186–3 and comments received on that draft are available electronically from the NIST Web site at: *http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html*, respectively. Comments received in response to this notice will be published electronically at *http://csrc.nist.gov/groups/ST/toolkit/digital_signatures.html*.

Authority: In accordance 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.

Executive Order 12866: This notice has been determined not to be significant for the purposes of Executive Order 12866.

Dated: November 5, 2008.

Patrick Gallagher,

Deputy Director.

[FR Doc. E8–26841 Filed 11–10–08; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcing a Meeting of the Information Security and Privacy Advisory Board

AGENCY: National Institute of Standards and Technology.

ACTION: Meeting notice.

SUMMARY: Pursuant to the Federal Advisory Committee Act, 5 U.S.C. App., notice is hereby given that the Information Security and Privacy Advisory Board (ISPAB) will meet Wednesday, December 3, 2008 from 8:30 p.m. until 5 p.m., Thursday, December 4, 2008, from 8:30 a.m. until 5 p.m., and Friday, December 5, 2008 from 8 a.m. until 5:15 p.m. All sessions will be open to the public. The Advisory Board was established by the Computer Security Act of 1987 (Pub. L. 100–235) and amended by the Federal Information Security Management Act of 2002 (Pub. L. 107–347) to advise the Secretary of Commerce and the Director of NIST on security and privacy issues pertaining to federal computer systems. Details regarding the Board's activities are available at *http://csrc.nist.gov/groups/SMA/ispab/index.html/.*

DATES: The meeting will be held on December 3, 2008 from 8:30 p.m. until 5 p.m., December 4, 2008 from 8:30 a.m. until 5 p.m. and December 5, 2008, from 8 a.m. until 5:15 p.m.

ADDRESSES: The meeting will take place at George Washington University Cafritz Conference Center 800 21st Street, NW., Washington, DC, Room 405, on December 3 and 4, 2008 and 3rd Floor Continental Ballroom on December 5, 2008.

FOR FURTHER INFORMATION CONTACT: Ms. Pauline Bowen, Board Secretariat, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899–8930, *telephone:* (301) 975–2938.

SUPPLEMENTARY INFORMATION:

Agenda:

—Welcome and Overview
—OMB Update
—USCERT and Einstein
—ID Management
—Privacy Technology Report
—Center for Strategic and International Studies (CSIS) Commission Briefing
—ISC2 Software Credentialing
—Metrics and FISMA 08
—ISPAB Work Plan Discussion
—SCADA Security
—Threat Analysis, IC to Civilian
—Panel—Cloud Computing—Basics
—Panel—Cloud Computing—Security Strengths and Challenges
—Panel—Virtualization—Basics
—Panel—Cloud Computing and Virtualization

Note that agenda items may change without notice because of possible unexpected schedule conflicts of presenters. The final agenda will be posted on the Web site indicated above.

Public Participation: The Board agenda will include a period of time, not to exceed thirty minutes, for oral comments and questions from the public (Thursday, December 5, 2008 at 3:45–4:15 p.m.). Each speaker will be limited to five minutes. Members of the public who are interested in speaking are asked to contact the Board Secretariat at the telephone number indicated above. In addition, written statements are invited and may be submitted to the Board at any time. Written statements should be directed to the ISPAB Secretariat, Information Technology Laboratory, 100 Bureau Drive, Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930. Approximately 15 seats will be available for the public and media on December 3 and 4, 2008 and approximately 200 seats will be available for the public and media on December 5, 2008.

Dated: November 5, 2008.

Patrick Gallagher,

Deputy Director.

[FR Doc. E8–26840 Filed 11–10–08; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–AV00

Atlantic Highly Migratory Species; Essential Fish Habitat

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Extension of comment period.

SUMMARY: In order to provide additional opportunities for the public, the Atlantic Regional Fishery Management Councils, the Atlantic and Gulf States Marine Fisheries Commissions, and other interested parties to comment on the Essential Fish Habitat Draft Amendment 1 to the 2006 Consolidated Highly Migratory Species (HMS) Fishery Management Plan (FMP), NMFS is extending the comment period for this action. On September 19, 2008, NMFS published a Notice of Availability (NOA) of a draft environmental impact statement and a fishery management plan amendment. Based on the September 19, 2008, notice, the comment period was scheduled to conclude on November 18, 2008. NMFS is now extending the comment period until December 12, 2008. Comments received by NMFS on the Draft Amendment will be used in the development of Final Amendment 1 to the 2006 Consolidated HMS FMP.

DATES: The deadline for comments on Draft Amendment 1 has been extended from November 18, 2008, as published on September 19, 2008 (73 FR 54384), to 5:00 p.m. on December 12, 2008.

ADDRESSES: Written comments on this action should be sent to Chris Rilling, Highly Migratory Species Management Division by any of the following methods:

• E–mail: *HMSEFH@noaa.gov*.

• Mail: 1315 East–West Highway, Silver Spring, MD 20910. Please mark the outside of the envelope ''Comments on EFH Amendment to HMS FMP.''

• Fax: 301–713–1917.

Copies of Draft Amendment 1 to the Consolidated HMS FMP are available from the HMS website under ''Breaking News'' at *http://www.nmfs.noaa.gov/sfa/hms/* or by contacting Chris Rilling (see **FOR FURTHER INFORMATION CONTACT**).

FOR FURTHER INFORMATION CONTACT: Chris Rilling or Sari Kiraly by phone at (301) 713–2347 or by fax at (301) 713–1917.

SUPPLEMENTARY INFORMATION: The Magnuson–Stevens Act (16 U.S.C. 1801