disposition of proprietary information disclosed under APO in accordance with 19 CFR 355.306. Timely written notification of return/destruction of APO materials or conversion to judicial protective order is hereby requested. Failure to comply with the regulations and the terms of an APO is a sanctionable violation.

This administrative review and this notice are in accordance with section 751(a)(1) of the Act (19 U.S.C. 1675(a)(1)) and 19 CFR 351.221.

Dated: December 8, 1998.

Joseph A. Spetrini,

Acting Assistant Secretary for Import Administration.

[FR Doc. 98–33212 Filed 12–14–98; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology (NIST)

Board of Overseers of the Malcolm Baldrige National Quality Award

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

ACTION: Request for nominations of members to serve on the Board of Overseers of the Malcolm Baldrige National Quality Award.

SUMMARY: NIST invites and requests nomination of individuals for appointment to Board of Overseers of the Malcolm Baldrige National Quality Award (Board). The terms of some of the members of the Board will soon expire. NIST will consider nominations received in response to this notice for appointment to the Committee, in addition to nominations already received.

DATES: Please submit nominations on or before January 11, 1999.

ADDRESSES: Please submit nominations to Harry Hertz, Director, National Quality Program, NIST, Building 101, Room A605, Gaithersburg, MD 20899. Nominations may also be submitted via FAX to 301–948–3716. Additional information regarding the Committee, including its charter, current membership list, and executive summary may be found on its electronic home page at: <http://www.quality.nit.gov/tos.htm>.

FOR FURTHER INFORMATION CONTACT: Harry Hertz, Director, National Quality Program and Designated Federal Official, NIST, Building 101, Room A531, Gaithersburg, MD 20899; telephone 301–975–2163; FAX—301–948–3716; or via e-mail at harry.hertznist.gov.

SUPPLEMENTARY INFORMATION:

I. Board of Overseers of the Malcolm Baldrige National Quality Award Information

The Board was established in accordance with 15 U.S.C. 3711a(d)(2)(B), pursuant to the Federal Advisory Committee Act (5 U.S.C. app. 2).

Objectives and Duties

1. The Board shall review the work of the private sector contractor(s), which assists the Director of the National Institute of Standards and Technology (NIST) in administering the Award. The Board will made such suggestions for the improvement of the Award process as it deems necessary.

2. The Board shall provide a written annual report on the results of Award activities to the Director of NIST, along with its recommendations for the improvement of the Award process.

3. The Board will function solely as an advisory committee under the Federal Advisory Committee Act.

4. The Board will report to the Director of NIST.

Membership

1. The Board will consist of approximately eleven members selected on a clear, standardized basis, in accordance with applicable Department of Commerce guidance, and for their preeminence in the field of quality management. There will be a balanced representation from U.S. service and manufacturing industries, education and health care. The Board will include members familiar with the quality improvement operations of manufacturing companies, service companies, small businesses, education, and health care. No employee of the Federal Government shall serve as a member of the Board of Overseers.

2. The Board will be appointed by the Secretary of Commerce and will serve at the discretion of the Secretary. The term of office of each Board member shall be three years. All terms will commence on January 1 and end on December 31 of the appropriate year.

Miscellaneous

1. Members of the Board shall serve without compensation, but may, upon request, be reimbursed travel expenses, including per diem, as authorized by U.S.C. 5701 et seq.

2. The Board will meet annually, except that additional meetings may be called as deemed necessary by the NIST Director or by the Chairperson. Meetings are one to two days in duration.

3. Board meetings are open to the public. Board members do not have access to classified or proprietary information in connection with their Board duties.

II. Nomination Information

1. Nominations are sought from the private sector as described above.

2. Nominees should have established records of distinguished service and shall be familiar with the quality improvement operations of manufacturing companies, service companies, small businesses, education, and health care. The category (field of eminence) for which the candidate is qualified should be specified in the nomination letter. Nominations for a particular category should come from organizations or individuals within that category. A summary of the candidate's qualifications should be included with the nomination, including (where applicable) current or former service on federal advisory boards and federal employment. In addition, each nomination letter should state that the person agrees to the nomination, acknowledge the responsibilities of serving on the Board, and will actively participate in good faith in the tasks of the Board. Besides participation at meetings, it is desired that members be able to devote the equivalent of seven days between meetings to either developing or researching topics of potential interest, and so forth, in furtherance of their Board duties.

3. The Department of Commerce is committed to equal opportunity in the workplace and seeks a broad-based and diverse Board membership.

Dated: December 9, 1998.

Robert E. Hebner,

Acting Deputy Director.

[FR Doc. 98–33166 Filed 12–14–98; 8:45 am]

BILLING CODE 3510–13–M

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 981028268–8268–01]

Announcing Approval of Federal Information Processing Standard 186–1, Digital Signature Standard, and Request for Comments

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

ACTION: Notice; Request for comments.

SUMMARY: The Secretary of Commerce approved an interim final standard, which will be known as Federal Information Processing Standard (FIPS) 186–1, Digital Signature Standard (DSS). This interim final standard allows for both the use of the Digital Signature Algorithm (DSA) and the American National Standards Institute X9.31 standard by federal organizations. The X9.31 standard describes the Rivest-Shamir-Adleman (RSA) digital signature technique.

This notice advises the public of the Secretary's decision and solicits comments from the public, academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations. These comments will assist NIST in making a recommendation to the Secretary regarding a final decision.

DATES: *Effective date:* December 15, 1998. *Comment Date:* Comments are due on or before March 15, 1999.

ADDRESSES: Comments should be sent to Information Technology Laboratory, Attn: DSS/X9.31 Comments, National Institute of Standards and Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD 20899–8970.

Comments may also be sent electronically to: ''FIPS186RSA@nist.gov''.

Specifications of the FIPS 186 are available electronically at: <http://csrc.nit.gov/fips/>

Ordering information for the ANSI X9.31 standard is available from American Bankers Assoc./DC, X9 Customer Service Dept., P.O. Box 79064, Baltimore, MD 21279–0064, telephone 1–800–338–0626.

FOR FURTHER INFORMATION CONTACT: Edward Roback, National Institute of Standards and Technology, 100 Bureau Drive Stop 8930, Gaithersburg, MD 20899–8930; telephone 301–975–3696 or via fax at 301–948–1233.

SUPPLEMENTARY INFORMATION: Under Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to approve standards and guidelines for the cost effective security and privacy of sensitive information processed by federal computer systems. On May 10, 1994, the Secretary of Commerce approved FIPS 186, ''Digital Signature Standard,'' which specifies a single technique for the generation and verification of digital signatures. Recently, another technique, known as RSA, was approved as the X9.31 standard [*X9.31–1998 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)]* by ANSI. A second standard, based upon a technique known as elliptic curve, is expected to be completed and approved by ANSI in the near future. Agencies have expressed considerable interest to NIST in using these technologies.

On May 13, 1997, NIST published a **Federal Register** notice soliciting comments on amending FIPS 186 to allow for the use of other techniques, specifically mentioning RSA and elliptic curve (but not with detailed specifications as now exist for RSA in the ANSI X9.31 standard). The public comments overwhelmingly supported revising FIPS 186 to include these additional algorithms. RSA, which has withstood widespread scrutiny by the cryptographic research community, is available in many commercial products. NIST believes it to be robust and sufficiently strong for use by federal agencies.

Following ANSI's recent approval of the ANSI X9.31 standard, the Secretary of Commerce approved an interim modification to FIPS 186 (FIPS 186–1) to approve use of the digital signature technique specified in X9.31 in addition to the algorithm currently specified in FIPS 186. The Secretary's decision revise the old FIPS 186 by adding the following statements into the new FIPS 186–1.

Add the following as the last sentences of the ''Applications'' paragraph: The technique specified in ANSI X9.31 may be used in addition to the Digital Signature Algorithm (DSA) specified herein.

Add the following as the last two sentences of the ''Implementations'' paragraph: Agencies are advised that separate keys should be used for signature and confidentiality purposes when using the X9.31 standard. This is because the RSA algorithm can be used for both data encryption and digital signature purposes.

To minimize any potential for spoofing digital signatures, keys used for signature purposes should not be recoverable. Using separate keys will allow agencies to recover confidentiality keys but not signature keys.

The standard has also been modified to reflect the availability of conformity testing for DSA implementations. (ANSI's conformity testing program for X9.31 implementations is not yet in place.) Minor language modifications (e.g., indicating that two algorithms are now approved) and other administrative updates have also been made to the standard.

Since ANSI's conformance testing program for the X9.31 standard is not yet in place, federal agencies are advised, in the interim, to acquire products that vendors hold out as in conformance with ANSI X9.31. Agencies will be advised by NIST when a conformance testing program is in effect.

Comments are sought by NIST so as to make a recommendation to the Secretary regarding a final FIPS.

Federal Information Processing Standards Publication 186–1

<Approval Dates> 1998

Announcing the Digital Signature Standard (DSS)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104–106), and the Computer Security Act of 1987 (Public Law 100–235).

Name of Standard: Digital Signature Standard (DSS).

Category of Standard: Computer Security, Cryptography.

Explanation: This Standard specifies algorithms appropriate for applications requiring a digital, rather than written, signature. A digital signature is represented in a computer as a string of binary digits. A digital signature is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified. An algorithm provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key which corresponds to, but is not the same as, the private key. Each user possesses a private and public pair. Public keys are assumed to be known to the public in general. Private keys are never shared. Anyone can verify the signature of a user by employing that user's public key. Signature generation can be performed only by the possessor of the user's private key.

A hash function is used in the signature generation process to obtain a condensed version of data, called a message digest (see Figure 1). The message digest is then input to the digital signature (ds) algorithm to generate the digital signature. The digital signature is set to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. The hash function is specified in a separate standard, the Secure Hash Standard (SHS), FIPS 180–1. FIPS approved ds algorithms must be implemented with the SHS. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data.

[Figure 1 not reproduced in this **Federal Register** notice.]

Approving Authority: Secretary of Commerce.

Maintenance Agency: U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL).

Applicability: This standards is applicable to all Federal departments and agencies for the protection of sensitive unclassified information that is not subject to section 2315 of Title 10, United States Code, or section 3502(2) of Title 44, United States Code. This standard shall be used in designing and implementing public-key based signature systems which Federal departments and agencies operate or which are operated for them under contract. Adoption and use of this standard is available to private and commercial organizations.

Applications: A digital signature (ds) algorithm authenticates the integrity of the signed data and the identity of the signatory. A ds algorithm may also be used in proving to a third party that data was actually signed by the generator of the signature. A ds algorithm is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication. The technique specified in ANSI X9.31 may be used in addition to the Digital Signature Algorithm (DSA) specified herein.

Implementations: A ds algorithm may be implemented in software, firmware, hardware, or any combination thereof. NIST is developing a validation program to test implementations for conformance to this standard. Currently, conformance tests for ANSI X9.31 have not been developed. These tests will be developed and made available in the future. Information about the planned validation program can be obtained from the National Institute of Standards and Technology, Information Technology Laboratory, Attn: DSS Validation, 100 Bureau Drive Stop 8930, Gaithersburg, MD 20899–8930.

Agencies are advised that separate keys should be used for signature and confidentiality purposes when using the X9.31 standard. This is because the RSA algorithm can be used for both data encryption and digital signature purposes.

Export Control: Implementations of this standard are subject to Federal Government export controls as specified in Title 15, Code of Federal Regulations, Parts 768 through 799. Exporters are advised to contact the Department of Commerce, Bureau of Export Administration for more information.

Patents: The algorithms in this standard may be covered by U.S. or foreign patents.

Implementation Schedule: This standard becomes effective <insert>.

Specifications: Federal Information Processing Standard (FIPS) 186–1 Digital Signature Standard (affixed).

Cross Index:

a. FIPS PUB 46–2, Data Encryption Standard.

b. FIPS PUB 73, Guidelines for Security of Computer Applications.

c. FIPS PUB 140–1, Security Requirements for Cryptographic Modules.

d. FIPS PUB 171, Key Management Using ANSI X9.17.

e. FIPS PUB 180–1, Secure Hash Standard.

Qualifications: The security of a digital signature system is dependent on maintaining the secrecy of users' private keys. Users must therefore guard against the unauthorized acquisition of their private keys. While it is the intent of this standard to specify general security requirements for generating digital signatures, conformance to this standard does not assure that a particular implementation is secure. The responsible authority in each agency or department shall assure that an overall implementation provides an acceptable level of security. This standard will be reviewed every five years in order to assess its adequacy.

Waiver Procedure: Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, United States Code. Waiver shall be granted only when:

a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system; or

b. Cause a major adverse financial impact on the operator which is not offset by Government wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made with required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions, 100 Bureau Drive Stop 8970, Gaithersburg, MD 20899–8970.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the **Federal Register**.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Sec. 552(b), shall be part of the procurement documentation and retained by the agency.

Where to Obtain Copies of the Standard: Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 186–1 (FIPSPUB186–1), and identify the title. When microfiche is desired, this should be specified. Prices are published by NTIS in current catalogs and other issuances. Payment may be made by check, money order, deposit account or charged to a credit card accepted by NTIS.

Dated: December 9, 1998.

Robert E. Hebner,

Acting Deputy Director.

[FR Doc. 98–33167 Filed 12–14–98; 8:45 am]

BILLING CODE 3510–CN–M