Entered this 3rd day of March, 2006.

Darryl W. Jackson,

Assistant Secretary of Commerce for Export Enforcement.

[FR Doc. 06–2359 Filed 3–10–06; 8:45 am]

BILLING CODE 3510–DT–M

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 051114299–5299–01]

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

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

ACTION: Notice; Request for Comments.

SUMMARY: This notice announces Draft Federal Information Processing Standard 186–3, Digital Signature Standard, for public review and comment. The draft standard, designated ''Draft FIPS 186–3,'' is proposed to revise and supersede FIPS 186–2.

FIPS 186, first published in 1994, specifies 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) adopt 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.

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 June 12, 2006.

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: *elaine.barker@nist.gov.*

The current FIPS 186–2 and its proposed replacement, Draft FIPS 186–3, are available electronically at *http://csrc.nist.gov/publications/fips/index.html* and *http://csrc.nist.gov/publications/drafts.html,* respectively. Comments received in response to this notice will be published electronically at *http://csrc.nist.gov/CryptoToolkit/tkdigsigs.html.*

FOR FURTHER INFORMATION CONTACT: Elaine Barker, Computer Security Division, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930, telephone (301) 975–2911.

SUPPLEMENTARY INFORMATION: FIPS 186, Digital Signature Standard (DSS), first issued in 1994, specified a single technique for the generation and verification of digital signatures. FIPS 186–1 adopted a second technique that was approved as ANS X9.31, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), by the American National Standards Institute (ANSI). FIPS 186–2 adopted a third technique that computed digital signatures using elliptic curve technology as specified in another ANSI standard, ANS X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA).

Digital signature algorithms require keys to generate secure signatures. With advances in technology, the size of these keys must be increased to provide adequate security. rDSA and ECDSA have been specified with sufficient flexibility to use various key sizes. DSA was specified for key sizes between 512 and 1024 bits. Key sizes below 1024 bits are currently not considered adequate. Therefore, the requirements for key sizes for DSA, as specified in FIPS 186–3, have been revised to include key sizes of 2048 and 3072 bits, in addition to the previously allowed 1024-bit key size. These key sizes provide security that is equivalent to the 80, 112 and 128-bit key sizes of symmetric key encryption algorithms such as TDEA (Triple Data Encryption Algorithm), as specified in NIST Special Publication 800–67, and AES (Advanced Encryption Standard), as specified in FIPS 197.

ANS X9.31, published in 1998, specifies the generation of keys and digital signatures for only an 80-bit security level. Draft FIPS 186–3 specifies criteria for the generation of keys and digital signatures for additional security levels.

Many cryptographic applications use the RSA algorithm that was specified in PKCS #1 and that was developed by RSA Security. PKCS #1 is considered to provide adequate security for Federal Government applications. Therefore, in the interests of providing interoperability, Draft FIPS 186–3 allows implementations of PKCS #1 in addition to that of ANS X9.31 and specifies criteria for the generation of keys for PKCS #1 digital signature applications; no provision is currently provided in PKCS #1 for the generation of digital signature keys.

ANS X9.62 was published in 1998 and is currently under revision. Other requirements have been added in Draft FIPS 186–3 to address deficiencies present in the current ANS X9.62; these additional requirements are consistent with the proposed ANS X9.62 revision.

FIPS 186–2 included several methods for random number generation for the 80-bit security level. Draft FIPS 186–3 includes a new random number generator that can be used to provide random numbers at multiple security levels. This random number generator is based on the Approved hash functions specified in FIPS 180–2, Secure Hash Standard.

Draft FIPS186–3 includes methods for the generation of domain parameters and digital signature keys. These methods are referenced by NIST Special Publication 800–56, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, for the generation of domain parameters and keys for key establishment.

Draft FIPS 186–3 requires that parties have various assurances when generating and verifying digital signatures. Methods for obtaining these assurances will be specified in a future publication to be issued in the NIST Special Publication (SP) series, SP 800–89, Recommendation for Obtaining Assurances for Digital Signature Applications.

Authority: NIST's activities to develop computer security standards to protect Federal sensitive (unclassified) systems are undertaken pursuant to specific responsibilities assigned to NIST in Section 5131 of the Information Technology Management Reform Act of 1996 (Pub .L. 104–106) and the Federal Information Security Management Act of 2002 (Pub. L. 107–347).

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

Dated: March 4, 2006.

William Jeffrey,

Director.

[FR Doc. E6–3521 Filed 3–10–06; 8:45 am]

BILLING CODE 3510–CN–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: Notice of meeting.

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 Tuesday, March 21, 2006, from 8:30 a.m. until 5 p.m., Wednesday, March 22, 2006, from 8:30 a.m. until 5 p.m. and Thursday, March 23, 2006 from 8:30 a.m. until 12 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/ispab/.*

DATES: The meeting will be held on March 21, 2006 and March 22, 2006, from 8:30 a.m. until 5 p.m. and March 23, 2006, from 8:30 a.m. until 12 p.m.

ADDRESSES: The meeting will take place at the Doubletree Hotel and Executive Meeting Center, 1750 Rockville Pike, Rockville, Maryland.

Agenda

—Welcome and Overview.
—Privacy Act Framework Effort.
—Briefing on Suite B Cryptography.
—IDA Report on NIAP.
—Briefing on Department of Homeland Security National Common Body of Knowledge Initiative.
—Briefing on Software Assurance.
—Briefing on Department of Transportation ''Real ID'' Project.
—Status Reports on ISPAB Work Plan Items.
—Agenda Development for June 2006 ISPAB Meeting.
—Wrap-Up.

Note that agenda items may change without notice because of possible unexpected schedule conflicts of presenters.

Public Participation: The Board agenda will include a period of time, not to exceed thirty minutes, for oral comments and questions from the public. 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 below. 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. It would be appreciated if 25 copies of written material were submitted for distribution to the Board and attendees no later than March 17, 2006. Approximately 15 seats will be available for the public and media.

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.

Dated: February 28, 2006.

William Jeffrey,

Director.

[FR Doc. E6–3520 Filed 3–10–06; 8:45 am]

BILLING CODE 3510–CN–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Announcement of the American Petroleum Institute's Standards Activities

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice of intent to develop or revise standards and request for public comment and participation in standards development.

SUMMARY: The American Petroleum Institute (API), with the assistance of other interested parties, continues to develop standards, both national and international, in several areas. This notice lists the standardization efforts currently being conducted by API committees. The publication of this notice by the National Institute of Standards and Technology (NIST) on behalf of API is being undertaken as a public service. NIST does not necessarily endorse, approve, or recommend the standards referenced.

ADDRESSES: American Petroleum Institute, 1220 L Street, NW., Washington, DC 20005; telephone (202) 682–8000, *http://www.api.org.*

FOR FURTHER INFORMATION CONTACT: All contact individuals listed in the **SUPPLEMENTARY INFORMATION** section of this notice may be reached at the American Petroleum Institute.

SUPPLEMENTARY INFORMATION:

Background

The American Petroleum Institute develops and publishes voluntary standards for equipment, materials, operations, and processes for the petroleum and natural gas industry. These standards are used by both private industry and by governmental agencies. All interested persons should contact the appropriate source as listed for further information.

Pipeline Committee

1165, 1st Edition: SCADA Display Standard.

1110, 5th Edition: Pressure Testing of Liquid Petroleum Pipelines.

1113, 4th Edition: Developing a Pipeline Supervisory Control Center.

FOR FURTHER INFORMATION CONTACT: Andrea Johnson, Standards Department, e-mail: *johnsona@api.org.*

Committee on Marketing

1631, 6th Edition: Interior Lining and Periodic Inspection of Underground Storage Tanks.

1637, 3rd Edition: Using the API Color-Symbol System to Mark Equipment and Vehicles for Product Identification at Service Stations and Distribution Terminals.

1646, 1st Edition: Safety Practices for Service Station Contractors.

16xx, 1st Edition: Recommended Practice for Tank Truck Handling of ULSD.

FOR FURTHER INFORMATION CONTACT: David Soffrin, Standards Department, e-mail: *soffrind@api.org.*

Committee on Refining

Inspection

510, 9th Edition: Pressure Vessel Inspection Code: Maintenance Inspection, Rating, Repair, and Alteration.

Pressure Vessel and Tanks

650, 11th Edition: Welded Steel Tanks for Oil Storage.

653, 4th Edition: Tank Inspection, Repair, Alteration, and Reconstruction.

Electrical Equipment

500, 3rd Edition: Recommended Practice for Classification of Locations