Dated: July 3, 2001.

Faryar Shirzad,

Assistant Secretary for Import Administration.

[FR Doc. 01–17371 Filed 7–10–01; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Computer System Security and Privacy Advisory Board; Request for Nominations

AGENCY: National institute of standards and technology, Commerce.

ACTION: Request for nominations of members to serve on the Computer System Security and Privacy Advisory Board.

SUMMARY: NIST invites and requests nominations of individuals for appointment to the Computer System Security and Privacy Advisory Board (CSSPAB). The terms of some of the members will soon expire. NIST will consider nominations received in response to this notice for appointment to the Board, in addition to nominations already received.

DATES: Please submit nominations on or before August 15, 2001.

ADDRESSES: Please submit nominations to Dr. Fran Nielsen, CSSPAB Secretary, NIST, 100 Bureau Drive, M.S. 8930, Gaithersburg, MD 20899–8930. Nominations may also be submitted via fax to 301–948–2733: CSSPAB Nominations.

Additional information regarding the Board, including its charter and current membership list, may be found on its electronic home page at: http://csrc.nist.gov/csspab/.

FOR FURTHER INFORMATION CONTACT: Dr. Fran Nielsen, CSSPAB Secretary and Designated Federal Official, NIST, 100 Bureau Drive, M.S. 8930, Gaithersburg, MD 20899–8930; telephone 301–975–3669; telefax: 301–926–2733; or via email at fran.nielsen@nist.gov.

SUPPLEMENTARY INFORMATION:

I. CSSPAB Information

Objectives and Duties

The CSSPAB was chartered by the Department of Commerce pursuant to the Computer Security Act of 1987 (Pub. L. 100–235). The objectives and duties of the CSSPAB are:

1. The Board shall identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy.

2. The Board shall advise the National Institute of Standards and Technology (NIST) and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems.

3. To report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

4. The Board will function solely as an advisory body, in accordance with the provisions of the Federal Advisory Committee Act.

Membership

The CSSPAB is comprised of twelve members, in addition to the Chairperson. The membership of the Board includes:

(1) Four members from outside the Federal Government eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

(2) Four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) Four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

Miscellaneous

Members of the CSSPAB are not paid for their service, but will, upon request, be allowed travel expenses in accordance with Subchapter I of Chapter 57 of Title 5, United States Code, while otherwise performing duties at the request of the Board Chairperson, while away from their homes or a regular place of business.

Meetings of the Board are two to three days in duration and are held quarterly. The meetings primarily take place in the Washington, DC metropolitan area, usually at the NIST headquarters in Gaithersburg, MD.

Board meetings are open to the public and members of the press usually attend. Members do not have access to classified or proprietary information in connection with their Board duties.

II. Nomination Information

Nominations are sought in all three categories described above, including a small business representative in the first category.

Nominees should have specific experience related to computer security or electronic privacy issues, particularly as they pertain to federal information technology. The category of membership 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. Also include (where applicable) current or former service on federal advisory boards and federal employment. Each nomination letter should state that the person agrees to the nomination, acknowledges the responsibilities of serving on the CSSPAB, and will actively participate in good faith in the tasks of the CSSPAB. Besides participation at meetings, it is desired that members be able to devote the equivalent of two days between meetings to developing draft issue papers, researching topics of potential interest, and so forth in furtherance of their Board duties.

Selection of CSSPAB members will not be limited to individuals who are nominated. Nominees must be U.S. citizens.

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

Dated: July 5, 2001.

Karen H. Brown,

Acting Director, NIST.

[FR Doc. 01–17296 Filed 7–10–01; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 981028268–1130–04]

RIN 0693–ZA23

Announcing Proposed Changes to Federal Information Processing Standard (FIPS) 186–2, Digital Signature Standard (DSS), and Request for Comments

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

ACTION: Request for comments.

SUMMARY: The Secretary of Commerce approved FIPS 186–2, Digital Signature Standard, in January 2000. NIST proposes two minor changes to this standard to enable federal agencies to make a smooth transition to the

acquisition of equipment implementing the algorithms specified in the standard. These adjustments do not change the technical cryptographic signature algorithm specifications.

Before recommending these minor changes to FIPS 186–2 to the Secretary of Commerce for approval, NIST invites review and comments by the public, private sector, and government organizations.

DATES: Comments on these proposed changes to FIPS 186–2, Digital Signature Standard, must be received on or before August 10, 2001.

SPECIFICATIONS: FIPS 186–2, Digital Signature Standard, is available through the NIST Computer Security Resource Center web page: http://csrc.nist.gov/publications/fips/index.html. Text for the proposed changes is available at http://csrc.nist.gov/publications/drafts.html.

ADDRESSES: Comments on the proposed changes to FIPS 186–2 may be sent either electronically to FIPS 186@nist.gov or by regular mail to: Chief, Computer Security Division, Information Technology Laboratory, ATTN: Comments on Changes to FIPS 186–2 Digital Signature Standard, 100 Bureau Drive, Stop 8930, National Institute of Standards and Technology, Gaithersburg, MD 20899–8930.

FOR FURTHER INFORMATION CONTACT: Ms. Elaine Barker, (301) 975–2911, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930.

SUPPLEMENTARY INFORMATION: In January 2000, the Secretary of Commerce approved FIPS 186–2, Digital Signature Standard (DSS). The standard adopts three techniques for the generation and verification of digital signatures. These are the Digital Signature Algorithm (DSA) and two techniques specified in industry standards (ANSI X9.31–1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry and ANSI 9.62, 1998 Public Key Cryptography for the Financial Services Industry: Elliptical Curve Digital Signature Algorithm). When the standard was approved, it provided for a transition period from July 2000 to July 2001 to enable federal agencies to continue to use their existing digital signature systems and to acquire additional equipment that might be needed to interoperate with these legacy digital signature systems. Several agencies have notified NIST that commercial equipment implementing another data formatting approach (as input to a signature algorithm) are more readily

available and that the original implementation schedule should be extended.

Therefore, NIST is proposing that the Implementation Schedule of FIPS 186–2 be modified to extend the transition period for the acquisition of equipment implementing FIPS 186–2 from July 2001 to December 2002. This will enable agencies to continue to acquire commercial products based on a private sector data formatting approach PKCS #1, which does not interoperate with the data formatting approach specified in FIPS 186–2. NIST believes that using the PKCS #1 is robust and sufficiently strong for use by federal agencies. Also NIST proposes that the Applications section of FIPS 186–2 be modified to clarify that implementations of PKCS #1 (version 1.5 or higher) may be used during the transition period. These proposed adjustments do not change the technical cryptographic digital signature specifications (other than data formatting) for the standard.

Authority: Under Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987 (Public Law 100–235), 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.

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

Dated: July 5, 2001.

Karen H. Brown,
Acting Director, NIST.
[FR Doc. 01–17297 Filed 7–10–01; 8:45 am]
BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

Notice of Government Owned Inventions Available for Licensing

AGENCY: National Institute of Standards and Technology, Commerce.
SUMMARY: The inventions listed below are owned in whole or in part by the U.S. Government, as represented by the Department of Commerce, and are available for licensing in accordance with 35 U.S.C. 207 and 37 CFR Part 404 to achieve expeditious commercialization of results of federally funded research and development.

FOR FURTHER INFORMATION CONTACT: Technical and licensing information on these inventions may be obtained by writing to: National Institute of Standards and Technology, Office of

Technology Partnerships, Building 820, Room 213, Gaithersburg, MD 20899; Fax 301–869–2751. Any request for information should include the NIST Docket No. and Title for the relevant invention as indicated below.

SUPPLEMENTARY INFORMATION: NIST may enter into a Cooperative Research and Development Agreement (''CRADA'') with the licensee to perform further research on the inventions for purposes of commercialization. The inventions available for licensing are:

NIST Docket Number: 00–018US.
Title: Inorganic Non-metallic, Wire Bondable Top Surface Coating For Use In wire Bonding To Copper Metallization On Semiconductor Chips.
Abstract: The invention addresses the problem of electrically interconnecting copper metallized semiconductor ships to their packages with wire bonding. A thin, inorganic film is deposited such that it will break-up during the wire bonding process and be pushed aside. Selected film materials are compatible with and normally used for other purposes in wafer fabrication processing.

NIST Docket Number: 97–017C.
Title: Domain Engineered Ferroelectric Optical Radiation.
Abstract: The invention comprises a pyroelectric detector with significantly reduced microphonic noise sensitivity comprising a pyroelectric detector element constructed from a z-cut LiNBO3 electret. Selective domain reversal is accomplished in the electret by applying an electric field. Electrodes are attached to either surface of the electret spanning the domain reversed region and a portion of the original domain region to create areas of equal and opposite sensitivity. The detector is mounted in an electrically grounded container or housing. The detector may also be constructed having multiple detector regions to accommodate resonant frequencies of the electret or to function as a position sensor.

NIST Docket Number: 9–026US–Transfer.
Title: Modular Suspended Manipulator.
Abstract: A Cable-driven manipulator can precisely manipulate tools and loads using position, velocity and force control modes. The manipulator includes a plurality of cables (2 or more) that are independently controlled by modular, winch drive mechanisms and is coordinated to achieve intuitive manipulator movement in all sex degrees of freedom. The manipulator, consisting of modular sub-assemblies and components (*i.e.,* winch, amplifier, servo interface and sensory feedback), can be rapidly reconfigured to adjust to new applications. The winches can be controlled manually by a multi-axis joystick, or can be automatically controlled by computer. the invention has applications in supporting and manipulating tools and equipment for welding, painting and stripping involving large structures.

NIST Docket Number: 99–035US.
Title: Normal Metal Boundary Conditions For Multi-layer TES Detectors.