DEPARTMENT OF COMMERCE

International Trade Administration

Applications for Duty-Free Entry of Scientific Instruments

Pursuant to section 6(c) of the Educational, Scientific and Cultural Materials Importation Act of 1966 (Pub. L. 89–651; 80 Stat. 897; 15 CFR part 301), we invite comments on the question of whether instruments of equivalent scientific value, for the purposes for which the instruments shown below are intended to be used, are being manufactured in the United States.

Comments must comply with 15 CFR 301.5(a)(3) and (4) of the regulations and be filed within 20 days with the Statutory Import Programs Staff, U.S. Department of Commerce, Washington, DC 20230. Applications may be examined between 8:30 a.m. and 5 p.m. in Room 4211, U.S. Department of Commerce, 14th Street and Constitution Avenue, NW, Washington, DC.

Docket Number: 99–020. Applicant: National Institutes of Health, National Institute on Deafness and Other Communication Disorders, 9000 Rockville Pike, Bethesda, MD 20892. *Instrument:* Electron Microscope, Model JEM–1010. *Manufacturer:* JEOL Ltd., Japan. *Intended Use:* The instrument is intended to be used for ultrastructural analyses of animal tissues using electron microscopy preparative techniques such as fixation, embedding and ultrathin sectioning and immunogold and other immunocytochemical techniques to localize cellular components and antigens and computerized imaging quantitation. In addition, the instrument will be used for training postdoctoral fellows and to some extent pre-IRTAs and students. *Application accepted by Commissioner of Customs:* August 25, 1999.

Docket Number: 99–021. *Applicant:* University of Kentucky, 177 Anderson Hall, Lexington, KY 40506–0046. *Instrument:* Electron Microscope, Model JEM–2010F. *Manufacturer:* JEOL Ltd., Japan. *Intended Use:* The instrument is intended to be used in the study of the structure and chemistry of a wide variety of materials in the solid state (e.g., polymers, ceramics, metals, superconductors, carbon nanotubes) with emphasis on the structure of material defects. Experiments will include: (1) Quantification of interfacial segregation in oxide ceramics and correlation of segregation with interface crystallography, (2) high-resolution imaging of carbon nanotubes, and (3) phase identification of catalysts. In addition, the instrument will be used to train graduate students in the theory of electron microscopy in the courses MSE 858 Material Characterization Techniques and MSE 666 Diffraction Methods in Materials Science. *Application accepted by Commissioner of Customs:* August 25, 1999.

Frank W. Creel,

Director, Statutory Import Programs Staff.

[FR Doc. 99–24074 Filed 9–14–99; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

International Trade Administration

Overseas Trade Missions

AGENCY: International Trade Administration, Department of Commerce.

ACTION: Notice.

SUMMARY: The Department of Commerce invites U.S. companies to participate in the following overseas trade missions to be held between September 1999 and April 2000. For a more complete description of the trade mission, obtain a copy of the mission statement from the Project Officer indicated below. The recruitment and selection of private sector participants for these missions will be conducted according to the Statement of Policy Governing Department of Commerce Overseas Trade Missions announced by Secretary Daley on March 3, 1997.

Coal Trade Mission, Los Angeles Export Terminal, Los Angeles, CA, Comision Federal de Electricidad, Mexico City, Mexico, Petacalco Power Plant, Lazaro Cardenas, Mexico, September 28–October 2, 1999, Recruitment closes September 17, 1999, For further information contact: Helen Burroughs, U.S. Department of Commerce, Tel: 202–482–4931, Fax: 202–482–0170 or 202–482–5361.

Agricultural Trade Mission—PERU, November 29–December 3, 1999, Recruitment closes November 10, 1999, For further information contact: U.S. Department of Commerce, Eduardo Torres, Tel: 559–325–1619, Fax: 559–325–1647 or Dale Wright, Tel: 916–498–5155, Fax: 916–498–5923.

Pet Products Trade Mission, Mexico City and Guadalajara, Mexico, December 1–7, 1999, Recruitment closes November 15, 1999, For further information contact: Edward Kimmel, U.S. Department of Commerce, Tel: 202–482–3640, Fax: 202–482–3422.

Healthcare Technologies Matchmaker, Milan, Italy and Madrid, Spain, February 28–March 3, 2000, Recruitment closes January 7, 2000, For further information contact: Yvonne Jackson, U.S. Department of Commerce, Tel: 202–482–2675, Fax: 202–482–0178.

Medical and Dental Devices, Medical Device Components, and Laboratory Instruments, Trade Mission to China, March 19–28, 2000, Recruitment closes February 15, 2000, For further information contact: Lauren Saadat, U.S. Department of Commerce, Tel: 202–482–4431, Fax: 202–482–0975.

Used Equipment Trade Mission, Peru and Ecuador, April 10–15, 2000, Recruitment closes March 1, 2000, For further information John Bodson, U.S. Department Commerce, Tel: 202–482–0601, Fax: 202–482–0304. For further information contact: Reginald Beckham, U.S. Department of Commerce, Tel: 202–482–5478, Fax: 202–482–1999.

Dated: September 8, 1999.

Tom Nisbet,

Director, Promotion Planning and Support Division, Office of Export Promotion Coordination.

[FR Doc. 99–23979 Filed 9–14–99; 8:45 am]

BILLING CODE 3510–DR–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 970725180–9196–03]

RIN No. 0693–ZA16

Request for Comments on the Finalist (Round 2) Candidate Algorithms for the Advanced Encryption Standard (AES)

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

ACTION: Notice; request for comments.

SUMMARY: A process to develop a Federal Information Processing Standard (FIPS) for an Advanced Encryption Standard (AES) specifying an Advanced Encryption Algorithm (AEA) has been initiated by the National Institute of Standards and Technology (NIST). In the Fall of 1998, NIST announced fifteen publicly submitted algorithms as candidates for the AES, and invites public review, comment, and analysis in order to narrow the field of candidates to (approximately) five or fewer finalists. During the Round 1 technical evaluation period, these fifteen candidates were subjected to extensive analysis and testing by the cryptographic community.

At the conclusion of Round 1, NIST took the following information into consideration: (1) The submitted (official) versions of the AES candidate algorithms, (2) Round 1 public comments, (3) papers and discussions at the Second AES Candidate Conference, (4) results of NIST efficiency and statistical analysis, and (5) other relevant data (e.g., presentations at the Sixth Fast Software Encryption Workshop, discussions on NIST's AES Electronic Discussion Forum, etc.). Using this information, NIST has selected the AES finalist candidate algorithms (''finalists''), which will be subjected to further analysis during Round 2 of the AES development effort. A list of the finalists, along with specifications and intellectual property information, is available at the AES home page, *http://www.nist.gov/aes.*

This notice announces the beginning of the Round 2 technical evaluation period for the AES finalists. Additionally, the notice solicits comments on the finalists from the general public, academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations. NIST will use these comments to select one or more of the finalists for inclusion in a draft Federal Information Processing Standards Publication (FIPS PUB), on which public comments will be invited via a future **Federal Register** announcement.

NIST's goal is that the AES will specify one or more unclassified, publicly disclosed encryption algorithm(s) available royalty-free worldwide that is (are) capable of protecting sensitive government information well into the next century.

DATES: Public comments for Round 2 are due May 15, 2000. Paper proposals for the Third AES Candidate Conference (which are also considered as public comments) are due to NIST by January 15, 2000. The Third AES Candidate Conference (AES3) is scheduled for April 13–14, 2000.

ADDRESSES: Comments and paper proposals should be sent electronically to *AESround2@nist.gov.* Alternatively, they may be sent to: Information Technology Laboratory Attn: AES Finalist Comments (Bldg. 820, Room 423), National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899–8930, U.S.A.

AES-related comments received in response to this notice will be made part of the public record. Papers proposed for presentation at AES3 will be posted on the AES home page *http://www.nist.gov/aes* prior to the beginning of AES3. All additional Round 2 comments will be made available at the AES home page shortly after the Round 2 comments period closes.

FOR FURTHER INFORMATION CONTACT: The AES home page *http://www.nist.gov/aes* has all current NIST information pertaining to the AES development effort. Recent results and ongoing discussions regarding the finalists and AES-related issues takes place at the AES Electronic Discussion Forum, *http://aes.nist.gov/aes/default.htm.* General questions may be directed to Edward Roback at (301) 975–3696, or *eroback@nist.gov.*

Technical questions may be made by contacting Jim Foti at (301) 975–5237, *jfoti@nist.gov,* or Elaine Barker at (301) 975–2911, *ebarker@nist.gov.*

Algorithm-specific questions should be directed to the algorithm's submitter. Contact information for the submitters is located on the AES home page.

SUPPLEMENTARY INFORMATION:

1. AES Finalist Candidate Algorithms

NIST has selected the AES finalists for Round 2. The list of finalists, along with their specifications and intellectual property statements, is available electronically at the AES home page. At that same location, NIST is also making available a document that presents the rationale for NIST's selection of the finalists.

The Round 1 candidate algorithms that were not selected for Round 2 are no longer part of the AES development effort, and, therefore, will not be selected for inclusion in the AES FIPS. Those algorithms (including the specifications and reference and optimized code) may or may not be in the public domain (this includes using the code for testing and research purposes), so algorithm implements, users, and others should be aware of the intellectual property status of each individual algorthm. When the algorithms were initially submitted before the start of Round 1, each submitter signed an intellectual property statement, part of which states that

> * * * If my algorithm * * * is not selected for inclusion in the FIPS (including those not selected for second round of public evaluation), I understand that all rights, including use rights of the reference and mathematically optimized implementations, revert back to the submitter (and other owner[s] as appropriate).

Please note that the selection of an algorithm as a finalist does *not* constitute endorsement by NIST of the algorithm or it security. Similarly, the non-selection of an algorithm is not necessarily to be taken as a statement about the algorithm's quality, security, efficiency, or other characteristics. Algorithms selected as finalists were determined to be more suitable for the proposed FIPS. For specific details on an algorithm and its particular security characteristics, one should consult the various Round 1 public comments that were submitted to NIST (available on the AES home page).

Although no formal process has been established to address minor modifications of the finalists that may become necessary, NIST reserves the right to work with the submitters of the finalists regarding any such modifications. NIST intends to do this in the most open and public manner possible. This is consistent with the made in the original call for candidate algorithms, to which all submitters agreed that

> * * * the U.S. Government may, during the course of the lifetime of the AES or during the FIPS public review process, modify the algorithm's specifications (e.g., to protect against a newly discovered vulnerability).

2. Availability of AES CD–3

All persons with AES CD–1 and CD–2 should be aware of potential intellectual property issues with implementing and using algorithms on those CDs, especially for those algorithms that were not selected for Round 2. Please see the note in Section 1, above.

In addition to making specifications available on the AES home page, during Round 2 NIST will make a CD–ROM available (to be designatede ''AES CD–3'') which contains the algorithm specifications, supporting documentation, and submitted code for the AES finalists. It is anticipated that this code will be different from the code provided before the start of Round 1 (e.g., updated to be more efficient, additional code for various platforms, etc.). The submitters of the AES finalists are being given one month from the start of Round 2 to provide NIST with any updated code.

AES CD–3 should be available approximately 2–3 months after the beginning of Round 2. When it is ready for distribution, NIST will re-activate the AES CD Request Form at *http://csrc.nist.gov/encryption/aes/round1/cdreq.htm.* To those people in the U.S. and Canada who received AES CD–2, *NIST will automatically send a copy of AES CD–3.* So, for those people, there will be no need to provide NIST with an additional CD–ROM request.

Since AES CD–3 will contain algorithm code, it will be subject to export control, and NIST will handle export requests approriately. For those people *outside* of the U.S. and Canada who received AES CD–2 (for whom an export license was granted), AES CD–3 will automatically be distributed *only after a new export license is granted and their copy of AES CD–2 is returned to NIST, as required by the conditions of the original export license.* Information on where to send AES CD–2 is posted on the AES CD Request Form mentioned above.

3. Comments Solicited on the AES Finalists

Written comments on the finalists are solicited by NIST in this Round 2 technical evaluation in order to help NIST select one or more algorithms for specification in a draft AES FIPS. To facilitate the review of the comments, NIST asks the submitters of comments to clearly indicate the algorithm(s) to which their comments apply. Also, as guidance to comment submitters, the original Evaluation Criteria published on September 12, 1997, are reproduced in Section 4 below.

NIST will accept both general comments and formal analyses/papers that will be considered for presentation at the Third AES Candidate Conference (see Section 5 below).

Since submitted comments will be made available to the public, the comments must not contain proprietary information.

Comments and analysis are sought on any aspect of the candidate algorithms, including—but not limited to—the following topics.

3.1 Cryptanalysis

Since *security* will be the most important characteristic of the selected algorithm(s), NIST strongly encourages and welcomes cryptanalysis of the finalists.

3.2 Intellectual Property of the AES Finalists

NIST seeks detailed comments regarding any intellectual property—particularly any patent not already identified by the finalists' submitters—that may be infringed by the practice of any of the finalists algorithms. This also includes comments from all parties—including submitters—regarding specific claims that the practice of a finalist algorithm infringes on their patent(s). Claims regarding infringement of copyrighted software are also particularly solicited. NIST views this input as a critical factor in the eventual widespread adoption and implementation of the algorithm(s) specified in the FIPS.

NIST reminds all interested parties that the adoption of AES is being conducted as an open standards-setting activity. Specifically, NIST has requested that all interested parties identify to NIST any patents or inventions that may be required for the use of AES. NIST hereby gives public notice that it may seek redress under the antitrust laws of the United States against any party in the future who might seek to exercise patent rights against any user of AES that have not been disclosed to NIST in response to this request for information.

3.3 Cross-Cutting Analyses of All of the AES Finalists

Public analysis comparing the entire field of finalists in a consistent manner for particular characteristics will be very useful. Examples of this type of analysis might include comparisons of the finalists regarding: (1) Performance on various smart cards, when the implementations are constructed to defend against timing and power analysis attacks, (2) performance and/or memory use measurements, when written in the same programming language, (3) relative performance on 64-bit processors, (4) performance of assembly language implementations on various platforms, and (5) performance of hardware implementations or simulations.

Additionally, surveys, analyses, and comments are invited regarding prospective future platforms and applications that will implement the AES FIPS algorithm(s).

During Round 2, NIST may take into consideration the issue of having ''variable rounds'' in the AES finalists. Therefore, NIST invites comments on how NIST should address the ''variable rounds'' issue during and after Round 2.

3.4 Overall Recommendations Regarding the Selection of the Algorithm(s) for the Proposed FIPS

When all factors are considered, which candidate algorithm(s) should be selected for inclusion in the FIPS? Also, conversely, NIST seeks the identification and justification of which algorithms should *not* be selected by NIST. Such comments (with supporting justifications) will be of great use to NIST and help assure timely progress of the AES selection process.

3.5 Related Recommendations Regarding Implementation of the AES FIPS

In addition to selecting the algorithm(s) to be included in the proposed FIPS, issues regarding the implementation requirements of the standard will also need to be addressed. Therefore, NIST is seeking comments (with rationale) on what requirements should be included in the FIPS. For example, if NIST selects multiple algorithms for inclusion in the proposed FIPS, should the standard require that products conforming to the FIPS implement (1) one algorithm, (2) two (or more) algorithms, (3) all algorithms, or (4) a varying number of algorithms, depending on the type of implementation (e.g., require all algorithms in software implementations, only one in hardware implementations, etc.)?

Also, upon final publication as a FIPS, NIST intends to provide validation testing for implementations of the AES algorithm(s), as it does with other FIPS-approved cryptographic algorithms. Comments pertaining to such validation testing are also welcome.

4. Evaluation Criteria

In the call for AES candidate algorithms (**Federal Register**, September 12, 1997, [Volume 62, Number 177], pages 48051–48058), NIST published evaluation criteria for use in reviewing candidate algorithms. For reference purposes, these criteria are reproduced below:

[Beginning of Excerpt]

Security (i.e., the effort required to cryptanalyze).

The security provided by an algorithm is the most important factor in the evaluation.

Algorithms will be judged on the following factors:

i. Actual security of the algorithm compared to other submitted algorithms (at the same key and block size).

ii. The extent to which the algorithm output is indistinguishable from a random permutation on the input block.

iii. Soundness of the mathematical basis for the algorithm's security.

iv. Other security factors rasied by the public during the evaluation process, including any attacks that demonstrate that the actual security of the algorithm is less than the strength claimed by the submitter.

Claimed attacks will be evaluated for practicality.

Cost

i. Licensing requirements: NIST intends that when the AES is issued, the algorithm(s) specified in the AES shall be available on a worldwide, non-exclusive, royalty-free basis.

ii. Computational efficiency: The evaluation of computational efficiency will be applicable to both hardware and software implementations. Round 1 analysis by NIST will focus primarily on software implementations and specifically on one key-block size combination (128–128); more attention will be paid to hardware implementations and other supported key-block size combinations (particularly those required in the ''Minimum Acceptability Requirements'' section) during Round 2 analysis.

Computational efficiency essentially refers to the speed of the algorithm. NIST's analysis of computational efficiency will be made using each submission's mathematically optimized implementations on the platform specified under ''Round 1 Technical Evaluation'' below. Public comments on each algorithm's efficiency (particularly for various platforms and applications) will also be taken into consideration by NIST.

iii. Memory requirements: The memory required to implement a candidate algorithm—for both hardware and software implementations of the algorithm—will also be considered during the evaluation process. Round 1 analysis by NIST will focus primarily on software implementations; more attention will be paid to hardware implementations during Round 2.

Memory requirements will include such factors as gate counts for hardware implementations, and code size and RAM requirements for software implementations.

Testing will be performed by NIST using the mathematically optimized implementations provided in the submission package. Memory requirement estimates (for different platforms and environments) that are included in the submission package will also be taken into consideration by NIST. Input from public evaluations of each algorithm's memory requirements (particularly for various platforms and applicants) will also be taken into consideration by NIST.

Algorithm and Implementation Characteristics

i. Flexibility: Candidate algorithms with greater flexibility will meet the needs of more users than less flexible ones, and, therefore, inter alia, are preferable. However, some extremes of functionality are of little practical application (e.g., extremely short key lengths)—for those cases, preference will not be given.

Some examples of ''flexibility'' may include (but are not limited to) the following:

a. The algorithm can accommodate additional key- and block-sizes (e.g., 64-bit block sizes, key sizes other than those specified in the Minimum Acceptability Requirements section, [e.g., keys between 128 and 256 that are multiples of 32 bits, etc.]).

b. The algorithm can be implemented securely and efficiently in a wide variety of platforms and applications (e.g., 8-bit processors, ATM networks, voice & satellite communications, HDTV, B-ISDN, etc.).

c. The algorithm can be implemented as a stream cipher, Message Authentication Code (MAC) generator, pseudo-random number generator, hashing algorithm, etc.

ii. Hardware and software suitability: A candidate algorithm shall not be restrictive in the sense that it can only be implemented in hardware. If one can also implement the algorithm efficiency in firmware, then this will be an advantage in the area of flexibility.

iii. Simplicity: A candidate algorithm shall be judged according to relative simplicity of design.

[End of excerpt]

5. Initial Planning for the Third AES Candidate Conference (AES3)

Near the end of Round 2, NIST will sponsor the Third AES Candidate Conference (AES3)—another open, public forum that will be used to discuss analyses of the AES finalists. Additionally, submitters of the AES finalists will be invited to attend and engage in discussions regarding comments on their algorithms.

AES3 will be held April 13–14, 2000, at the Hilton New York and Towers, in New York City. The AES home page contains registration and logistical information, in addition to information on other nearby hotels. As for AES2 (March 22–23, 1999), AES3 will be held during the same week and at the same location as the Fast Software Encryption (FSE) Workshop (a link to FSE information will be available on the AES home page).

Paper submissions for AES3 should be sent to *AESround2@nist.gov* as an official comment, with a note indicating that the paper is being submitted for AES3. The deadline for AES3 submissions is January 15, 2000. All papers must be submitted in one of the following formats: Adobe PDF, Postscript, Rich Text Format (RTF), or Microsoft Word97. (For Adobe PDF and Postscript submissions, please embed all necessary fonts within the document.) All papers received for AES3—regardless of their acceptance for presentation at AES3—will be made available on the AES home page prior to the conference.

Appreciation

NIST extends its appreciation to *all* AES candidate algorithm submitters—both those submitters whose algorithms did and did not quality for Round 2—and those people providing public comments during the AES development process.

Dated: September 9, 1999.

Karen Brown,

Deputy Director, NIST.

[FR Doc. 99–24014 Filed 9–14–99; 8:45 am]

BILLING CODE 3510–CN–M′

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

National Marine Sanctuary Program

AGENCY: Office of Ocean and Coastal Resource Management (OCRM), National Ocean Service (NOS), National Oceanic and Atmospheric Administration (NOAA), Department of Commerce (DOC).

ACTION: Notice.

SUMMARY: NOAA is withdrawing the Northwest Straits from consideration as an Active Candidate for designation as a National Marine Sanctuary. The Northwest Straits are located north of Puget Sound, and encompass marine waters surrounding the San Juan Islands, north to the Canadian border, U.S. waters west to the entrance of the Strait of Juan de Fuca, Haro and Rosario Straits and the lower portion of the Strait of Georgia. The Northwest Straits site was identified by NOAA for evaluation as a national marine sanctuary by being listed on the National Marine Sanctuary Program's Site Evaluation List (SEL) in 1983 (as ''Washington State Nearshore''). Congress directed NOAA to prepare a designation prospectus on Northwest Straits in 1988 and the site became an Active Candidate. For reasons related to designation guidance contained in the 1996 reauthorization of the National Marine Sanctuary Act (NMSA), the findings of a Congressionally-convened Northwest Straits Citizens Advisory Commission, and limited agency resources, NOAA is discontinuing consideration of the site for possible designation as a national marine sanctuary.

FOR FURTHER INFORMATION CONTACT: Debra Malek, NOAA Marine Sanctuaries Division, 1305 East-West Highway, N/ORM2, Silver Spring, Maryland 20910 or at (301) 713–3141 Ext. 162.

SUPPLEMENTARY INFORMATION:

I. Background

The NMSA (16 U.S.C. 1431 *et seq.*) authorizes the Secretary of Commerce to designate discrete areas of the marine environment as national marine sanctuaries to fulfill the purposes and policies of the NMSA (set forth in section 301(b) (16 U.S.C. 1431(b)), and if: (1) the area proposed for designation is of special national significance due to its resource or human-use values; (2) existing state and federal authorities are inadequate or should be supplemented to ensure coordinated and comprehensive conversation and management of the area, including resource protection, scientific research, and public education; (3) designation of the area as a national marine sanctuary will facilitate the coordinated and comprehensive conservation and management of the area; and (4) the area is of a size and nature that will permit comprehensive and coordinated conservation and management (16