SUMMARY: The Secretary of Commerce issued an export trade certificate of review to J.J. Wheeling (d/b/a Aidex). Because this certificate holder has failed to file an annual report as required by law, the Department is initiating proceedings to revoke the certificate. This notice summarizes the notification letter sent to J.J. Wheeling (d/b/a Aidex).

FOR FURTHER INFORMATION CONTACT: Morton Schnabel, Director, Office of Export Trading Company Affairs, International Trade Administration, (202) 482–5131. This is not a toll-free number.

SUPPLEMENTARY INFORMATION: Title III of the Export Trading Company Act of 1982 (''the Act'') [15 U.S.C. 4011–21] authorizes the Secretary of Commerce to issue export trade certificates of review. The regulations implementing Title III (''the Regulations'') are found at 15 CFR part 325. Pursuant to this authority, a certificate of review was issued on May 13, 1992 to J.J. Wheeling (d/b/a Aidex).

A certificate holder is required by law (Section 308 of the Act, 15 U.S.C. 4018) to submit to the Department of Commerce annual reports that update financial and other information relating to business activities covered by its certificate. The annual report is due within 45 days after the anniversary date of the issuance of the certificate of review (Sections 325.14(a) and (b) of the Regulations). Failure to submit a complete annual report may be the basis for revocation. (Sections 325.10(a) and 325.14(c) of the Regulations).

The Department of Commerce sent to J.J. Wheeling (d/b/a Aidex), on May 3, 1998, a letter containing annual report questions with a reminder that its annual report was due on June 27, 1998. Additional reminders were sent on July 1, 1998, and on July 27, 1998. The Department has received no written response to any of these letters.

On August 27, 1998, and in accordance with Section 325.10 (c)[1] of the Regulations, a letter was sent by certified mail to notify J.J. Wheeling (d/b/a Aidex) that the Department was formally initiating the process to revoke its certificate. The letter stated that this action is being taken because of the certificate holder's failure to file an annual report.

In accordance with Section 325.10(c)[2] of the Regulations, each certificate holder has thirty days from the day after its receipt of the notification letter in which to respond. The certificate holder is deemed to have received this letter as of the date on which this notice is published in the **Federal Register**. For good cause shown, the Department of Commerce can, at its discretion, grant a thirty-day extension for a response.

If the certificate holder decides to respond, it must specifically address the Department's statement in the notification letter that it has failed to file an annual report. It should state in detail why the facts, conduct, or circumstances described in the notification letter are not true, or if they are, why they do not warrant revoking the certificate. If the certificate holder does not respond within the specified period, it will be considered an admission of the statements contained in the notification letter (Section 325.10(c)[2] of the Regulations).

If the answer demonstrates that the material facts are in dispute, the Department of Commerce and the Department of Justice will, upon request, meet informally with the certificate holder. Either Department may require the certificate holder to provide the documents or information that are necessary to support its contentions (Section 325.10(c)[3] of the Regulations).

The Department will publish a notice in the **Federal Register** of the revocation or modification or a decision not to revoke or modify (Section 325.10(c)[4] of the Regulations). If there is a determination to revoke a certificate, any person aggrieved by such final decision may appeal to an appropriate U.S. district court within 30 days from the date on which the Department's final determination is published in the **Federal Register** (Sections 325.10(c)(4) and 325.11 of the Regulations).

Dated: September 3, 1998.

Morton Schnabel,

Director, Office of Export Trading Company Affairs.

[FR Doc. 98–24559 Filed 9–11–98; 8:45 am]

BILLING CODE 3510–DR–P

DEPARTMENT OF COMMERCE

International Trade Administration

Environmental Technologies Trade Advisory Committee (ETTAC)

AGENCY: International Trade Administration, US Department of Commerce.

ACTION: Notice of open meeting.

SUMMARY: The Environmental Technologies Trade Advisory Committee will hold a plenary meeting from 8:30 AM until 11:30 PM on September 17, 1998. The ETTAC was created on May 31, 1994, to advise the U.S. government on policies and programs to expand U.S. exports of environmental products and services.

DATE AND PLACE: September 17, 1998; Room 3407 of the Department of Commerce, 14th Street and Constitution Avenue, NW, Washington, DC 20230.

The plenary meeting will review the objectives and agendas of its five subcommittee working groups: Market Access, Trade Impediments, Government Resources, Finance, and Outreach. There will also be an update on the APEC trade liberalization process, and updates from Environmental Trade Working Group members.

This meeting is physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Sage Chandler, Department of Commerce, Office of Environmental Technologies Exports. Phone: 202–482–1500

Dated: September 4, 1998.

Carlos Montoulieu,

Acting Deputy Assistant Secretary, Office of Environmental Technologies Exports.

[FR Doc. 98–24620 Filed 9–11–98; 8:45 am]

BILLING CODE 3510–DR–M

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 970725180–8168–02]

RIN 0693–ZA16

Request for Comments on 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 Advanced Encryption Standard (AES) specifying an Advanced Encryption Algorithm (AEA) has been initiated by the National Institute of Standards and Technology (NIST). Earlier this year, candidate algorithms were nominated to NIST for consideration for inclusion in the AES. Those candidate algorithms meeting the minimum acceptability criteria have been announced by NIST and are available electronically at the address listed below.

This notice solicits comments on the candidate algorithms from the public, and academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations. These comments will assist NIST in narrowing the field of AES candidates to five or fewer for more detailed examination.

It is intended that the AES will specify an unclassified, publicly disclosed encryption algorithm available royalty-free worldwide that is capable of protecting sensitive government information well into the next century.

DATES: Public comments are due April 15, 1999.

Authors who wish to be considered to be invited to brief their papers at the Second AES Candidate Conference must submit their papers by February 1, 1999.

ADDRESSES: Comments on the candidate algorithms should be sent to Information Technology Laboratory, Attn: AES Candidate Comments, Building 820, Room 562, National Institute of Standards and Technology, Gaithersburg, MD 20899.

Comments may also be sent electronically to AESFIRSTROUND@NIST.GOV

Specifications of the candidate algorithms are available electronically at <http://csrc.nist.gov/encryption/aes/aes__home.htm> as if information on how to obtain software implementations of the candidate algorithms (for evaluation and analysis purposes) and information on the Second AES Candidate Conference.

Comments received in response to this notice will be made part of the public record and will be made available for inspection and copying in the Central Records and Reference Inspection Facility, Room 6020, Herbert C. Hoover Building, 14th Street between Pennsylvania and Constitution Avenues, NW, Washington, DC, 20230.

Electronic comments received by NIST will be made available electronically at <http://csrc.nist.gov/encryption/aes/aes__home.htm>

FOR FURTHER INFORMATION CONTACT: For general information, contact: Edward Roback, National Institute of Standards and Technology, Building 820, Room 426, Gaithersburg, MD 20899; telephone 301–975–3696 or va fax at 301–948–1233.

Technical questions may be made by contacting either Miles Smid at (301) 975–2938, or Jim Foti at (301) 975–5237.

SUPPLEMENTARY INFORMATION:

I. Availability of AES Candidate Algorithm Specifications/Implementations

Specifications of the candidate algorithms are available electronically at <http://csrc.nist.gov/encryption/aes/aes__home.htm>. That site also contains information on ordering two CDROMs containing the AES candidate-related information. The first CDROM contains the same descriptions of the algorighm candidates available on the web site. The second CDROM contains the ANSI C and Java™ referenced and optimized implementations which are available for algorithm testing purposes.

The second CDROM (candidate algorithm implementations) is subject to U.S. export controls for destinations outside the U.S. and Canada. Information is available on the web site regarding how interested parties outside the U.S. and Canada can obtain a copy of the second CDROM.

Note that, with a few exceptions, the submitters of candidate algorithms have only made their candidate algorithms publicly available for AES testing and evaluation purposes. Unless otherwise specified by the submitter, these algorithms are protected and may not be otherwise used (e.g., in commercial or non-commercial products).

II. Comments Solicited on AES Candiate Algorithms

Written comments on the candidate algorithms are solicited by NIST in this ''Round 1'' technical evaluation in order to help NIST reduce the field of AES candidates to five or fewer for the ''Round 2'' technical analysis. It is envisioned that this narrowing will primarily be based on security, efficiency, and intellectual property considerations. Comments are specifically sought on: (1) specific security, efficiency, intellectual property, and other aspects of individual AES candidate algorithms; and, (2) cross-cutting analyses of all candidates. As discussed below, NIST particularly would appreciate receiving recommendations (with supporting justification) for the specific five (or fewer) algorithms which should be considered for Round 2 analysis. To facilitate review of the comments, it would be useful if those submitting comments would clearly indicate the particular algorithm(s) to which their comments apply.

NIST will accept both: 1) general comments; and, 2) formal analysis/papers which will be considered for presentation at the ''Second AES Candidate Conference.''

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

Comments and analysis are sought on any aspect of the candidate algorithms, including, but not limited to:

1. Comments on Candidate Algorithms Based Upon AES 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 are reproduced below. Comments are sought on the candidate algorithms and all aspects of the evaluation criteria.

Evaluation Criteria (as published September 12, 1997).

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 raised by the public during the evaluation process, including any attacks which 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 Requirement 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 applications) 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 the 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 efficiently 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.

2. Intellectual Property

Comments are also sought specifically regarding any patents (particularly any not otherwise identified by the submitter of each candidate) that may be infringed by the practice of each nominated candidate algorithm.

3. Cross-Cutting Analyses

Analysis comparing the entire field of candidates in a consistent manner for particular characteristics would be useful. Example of this type of analysis might include: (1) Comparisons of implementations of all algorithms written in the same programming language for memory use, timings for encryption/decryption/key setup/key change, and so forth; (2) comparisons of all algorithms against a particular cryptologic attack; or (3) comparison of all algorithms for infringement against a particular patent.

4. Overall Recommendations

When all factors are considered, which candidate algorithms should be selected for the next round of evaluation and why? (Since NIST intends to select five or few algorithms for Round 2, it would be useful to identify five or fewer in this regard.) Also, conversely, identification and justification of which algorithms should NOT be selected for the next round of evaluation. Such comments (with supporting justifications) will be of great use to NIST and help assure timely progress of the AES selection process.

III. Initial Planning for the Second AES Candidate Conference

An open public conference is being planned for the spring of 1999 to discuss analyses of the candidate algorithms. Those individuals who have submitted particularly insightful and useful comments may be invited by NIST to present their papers at the conference. Panels may also be organized around individual algorithms or cross-cutting analysis topics. Also, submitters of candidate algorithms will be invited to attend and engage in discussions responding to comments regarding their candidates. Because of the anticipated volume of comments, not all authors of comments can be invited to participate on the official program. At the conference, NIST intends to provide a briefing of the results of its efficiency testing of the candidate algorithm implementations, along with any other testing it may have completed.

In order to allow for timely conference preparation, authors who wish to be considered on the official program of the Second AES Candidate Conference must have their papers submitted to NIST by February 1, 1999. (They are to be sent to the same address as the general comments but should also be annotated as ''conference paper candidate.'' They will automatically be entered into the public record of AES candidate comments.)

As details and registration procedures are finalized, they will be posted to <http://csrc.nist.gov/encryption/aes/aes__home.htm>.

IV. General AES Development Information

For information regarding NIST's plans to test the candidate algorithms, the overall AES selection process, and the call for candidate algorithms, see NIST's notice in the **Federal Register**, September 12, 1997 (Volume 62, Number 177), pages 48051–48058, ''Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES).''

Appreciation

NIST extends its appreciation to all submitters and those parties providing public comments during the AES development process.

Dated: September 4, 1998.

Robert E. Hebner,

Acting Deputy Director.

[FR Doc. 98–24560 Filed 9–11–98; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

Modernization Transition Committee (MTC) Meeting

ACTION: Notice of public meeting.

TIME AND DATE: September 30, 1998, beginning at 8 a.m.

PLACE: This meeting will take place at the Silver Spring Holiday Inn, 8777 Georgia Avenue, Silver Spring, Maryland.

STATUS: The meeting will be open to the public. The time between 11 a.m. and 12 noon will be set aside for public comments. Approximately 50 seats will be available to the public on a first-come first-served basis.

MATTERS TO BE CONSIDERED: This meeting will include MTC consultation on the proposed Consolidation, Automation and Closure Certifications for Charlotte, North Carolina, Fort Wayne and South Bend, Indiana, and Victoria, Texas; presentation on NWS Severe Weather Performance in 1998; a status update on Evansville; and a report on the National Weather Service Modernization status.

FOR FURTHER INFORMATION CONTACT:

Nicholas Scheller, National Weather Service, Modernization Staff, 1325 East-West Highway, SSMC2, Silver Spring, Maryland 20910. Telephone: (301) 713–0454.

Dated: September 4, 1998.

John J. Kelly, Jr.,

Assistant Administrator for Weather Services.

[FR Doc. 98–24610 Filed 9–11–98; 8:45 am]

BILLING CODE 3510–12–M