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