DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 970725180–7180–01]

RIN No. 0693–ZA16

Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard

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

ACTION: Notice; Request for candidate encryption algorithm nomination packages.

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). This notice requests submission of candidate algorithms for consideration for inclusion in the AES and specifies how to submit a nomination package. The requirements for candidate algorithm submission packages and minimum acceptability requirements that must be satisfied in order to be deemed a ''complete and proper'' submission are presented. the evaluation criteria which will be used to appraise the candidate algorithms are also described.

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.

The purpose of this notice is to solicit candidate algorithms from the public, academic/research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations. Following the close of the submission period, NIST intends to make all submissions publicly available for review and comment.

DATES: *Submission deadline:* Candidate algorithm nomination packages must be received by June 15, 1998.

Submission packages received before April 15, 1998, will be reviewed for completeness by NIST and notified of their specific deficiencies, if any, by May 15, 1998, allowing time for deficient packages to be amended by the submission deadline.

No amendments to deficient packages will be permitted after the submission deadline. Requests for withdrawal of candidate algorithm submission packages previously submitted will only be honored until the submission deadline.

ADDRESSES: Candidate algorithm submission packages should be send to Director, Information Technology Laboratory, Attn: Advanced Encryption Standard Nominations, Technology Building, Room A231, National Institute of Standards and Technology, Gaithersburg, MD 20899.

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 via fax at 301–948–1233.

If necessary, general questions for clarification of these requirements for candidate algorithm submission packages, minimum acceptability requirements, or evaluation criteria/process should be sent electronically to AESQUEST@NIST.GOV or via fax to 301–948–1233 (Attn: AES Questions). In fairness to all parties, answers to germane questions will be made publicly available simultaneously to all those interested at <http://csrc.nist.gov/encryption/aes>. Non-pertinent questions may be ignored.

Technical questions and questions related to a specific submission package may be made by contacting either Miles Smid at (301) 975–2938, or Jim Foti at (301) 975–5237.

NIST will endeavor to answer all questions in a timely manner.

SUPPLEMENTARY INFORMATION: This section contains the following:

1. Background

This work effort is being initiated pursuant to NIST's responsibilities under the Computer Security Act of 1987, the Information Technology Management Reform Act of 1996, Executive Order 13011, and OMB Circular A–130.

NIST recognizes that many institutions, both within and outside the Federal Government, have considerable investments in their current installed base of encryption equipment implementing the Data Encryption Algorithm, specified in the Data Encryption Standard (DES, Federal Information Processing Standard 46–2). DES was first approved in 1977 and was most recently reaffirmed by the Secretary in 1993, until December 1998. In 1993 the following statement was included in the standard:

> At the next review (1998), the algorithm specified in this standard will be over twenty years old. NIST will consider alternatives which offer a high level of security. One of these alternatives may be proposed as a replacement standard at the 1998 review.

It is NIST's view that a multi-year transition period will be necessary to move toward any new encryption standard and the DES will continue to be of sufficient strength for many applications. NIST will consult with all interested parties so that a smooth transition can be accomplished. NIST may not complete the AES selection process before the end of its 1998 DES Review, and an interim solution(s) may be necessary.

For interoperability and other purposes, NIST strongly desires to select a single block encryption algorithm to be specified in the AES with a strength equal to or better than that of Triple DES and significantly improved efficiency. However, if more than one suitable candidate is identified which provides significantly better advantages in a specific application(s), NIST may consider recommending more than one algorithm. Present resource constraints do not permit the development of a specific standard algorithm for 8-bit smart card implementations or a standard stream cipher. It is hoped that the block cipher selected will be suitably flexible for a wide variety of implementations, recognizing that it may not operate with optimal efficiency in each and every potential application.

2. Requirements for Candidate Algorithm Submission Packages

To be considered as a ''complete'' nomination package (and continue further in the AES consideration process), candidate algorithm submission packages MUST contain the following (as described in detail below):

Cover sheet

Algorithm Specifications and Supporting Documentation

Magnetic media

Intellectual property statements/agreements/disclosures

Each of these is discussed in detail below, including ''general submission requirements'' which all nominations must also satisfy.

2. A Cover sheet

A cover sheet containing the following information:

Name of submitted algorithm
Principal submitter's name, telephone, fax, organization, postal address, e-mail address
Name(s) of auxiliary submitter(s)
Name of algorithm inventor(s) developer(s)
Name of owner, if any, of the algorithm. (normally expected to be the same as the submitter)
Signature of Submitter (optional)
Backup point of contact (w/telephone, fax, postal address, e-mail)

2.B Algorithm Specifications and Supporting Documentation

2.B.1 A complete written specification of the algorithm shall be included, consisting of all necessary mathematical equations, tables, diagrams, and parameters that are needed to implement the algorithm. The submission of all design rationale (e.g., method for generating table values, rationale for number of rounds, etc.) is strongly encouraged, in order to facilitate the public evaluation process.

Parity bits shall not be specified in the key definition. The bit naming/numbering convention for the key shall be provided by the submitter.

2.B.2 A statement of the algorithm's estimated computational efficiency in hardware and software shall be included. At a minimum, the submitter shall state efficiency estimates for the ''NIST AES analysis platform'' (specified elsewhere in section 6.B) and for 8-bit processors. (Efficiency estimates for other platforms may be included at the submitters' discretion.) These estimates shall *each* include the following information, at a minimum:

a. Description of the platform used to generate the estimate, in sufficient detail so that the estimates could be verified in the public evaluation process (e.g., for software running on a PC, include processor, clock speed, memory, operating system, etc.). For hardware estimates, it is encouraged that a gate count (or estimated gate count) be included.

b. Speed estimate for the algorithm on the platform specified in section 6.B. At a minimum, the number of clock cycles required to

(1) encrypt one block of data,
(2) decrypt one block of data,
(3) setup a key,
(4) setup the algorithm (e.g., build internal tables), and
(5) change a key after its initial setup

shall be specified *for each key- and block-size combination required in the Minimum Acceptability Requirements section of this announcement.*

c. Any available information on tradeoffs between speed and memory.

2.B.3 A series of Known Answer Tests (KATs) and Monte Carlo Tests (MCTs) shall be included as specified below. All of these KAT and MCT values shall be submitted electronically, in separate files, on a diskette as described in section 2.C.3. (The files containing test values may be compressed using PKZIP or GNUZIP to conserve disk space.) Each file shall be clearly labeled with header information listing: (1) Algorithm name, (2) Test name, (3) Description of the test, and (4) Key-block size combination being tested. All values within the file shall be clearly labeled (e.g., index, key, plaintext, ciphertext, etc.), and shall be in the exact format specified by NIST on its WWW site at <http://csrc.nist.gov/encryption/aes>.

a. All applicable KATs shall be included that can be used to exercise various features of the algorithm when operated in the Electronic Codebook (ECB) mode. A set of KATs shall be included for *each* key and block size specified in the Minimum Acceptability Requirements section. Required KATs include:

i. *Variable Key Known Answer Test*—A variable key KAT is required for the algorithm's encryption state. For an *n*-bit *key* size, there shall be *n* key-plaintext-ciphertext triples. The plaintext shall always consist entirely of binary zeros; the key shall always contain a single '1' bit and *n*-1 '0' bits, and the *n* possible keys (where each key has the '1' bit in a different position) shall be used to generate ciphertext. (To run this test for decryption, the ciphertext should be used as input to recover the block of all zero bits, for *each* possible one-bit key.)

ii. *Variable Plaintext Known Answer Test*—A variable plaintext KAT is required for the algorithm's encryption state. For an *m*-bit *block* size, there shall be *m* kep-plaintext-ciphertext triples. The key shall always consist entirely of binary zeros; the plaintext block shall always contain a single '1' bit and *m*-1 '0' bits, and the *m* possible blocks (where each input block has the '1' bit in a different position) shall be used to generate ciphertext. (To run this test for decryption, the ciphertext should be used as input to recover the correct input block, using the key consisting only of '0' bits.)

iii. If the candidate algorithm calculates intermediate values (e.g., internal rounds) for an encryption or decryption operation, then the submitter shall include known answers for those intermediate values for a single encryption and decryption operation for *each* of the required key- and block-size combinations.

iv. If tables are used in the algorithm, then a known answer test shall be included to exercise every table entry.

Note: The submitter may include any other known answer tests that exercise different features of the algorithm (e.g., for permutation tables, etc.). The purposes of these tests shall be clearly described in the file containing the test values.

b. Four Monte Carlo Tests shall be included, with key and data values, for *each* of the key-block combinations required in the Minimum Acceptability Requirements section. These four tests correspond with tests specified in the NIST Special Publication, *Modes of Operation Validation System: Requirements and Procedures* [MOVS]. The four tests required for the AES submissions correspond with the two Electronic Codebook Modes Tests for encryption and decryption (Sections 5.1.1.5 and 5.1.2.5 in [MOVS]) the two Cipher Block Chaining Modes Tests for encryption and decryption (Sections 5.2.1.5 and 5.2.2.5 in [MOVS]).

A link to a description of the required tests will be available at <http://csrc.nist.gov/encryption/aes>. Required submission data for the Monte Carlo Tests will also be found at that location.

2.B.4 A statement of the expected strength (i.e. workfactor) of the algorithm shall be included, along with any supporting rationale. The expected strength shall be given for *each* key- and block-size combination required in the minimum Acceptability Requirements section of this announcement, and for all other key- and block-size combinations claimed to be supported by the algorithm.

2.B.5 An analysis of the algorithm with respect to known attacks (e.g., known and chosen plaintext) shall be included. In addition, all known weak keys, equivalent keys, complementation properties, restrictions on key selection, and other similar features of the algorithm shall be noted by the submitter. If no such values are known, then this shall be stated by the submitter.

The submitter should provide any mathematical rationale for the non-existence of ''trap-doors'' in the algorithm, to the greatest extent possible.

The submitter shall provide a list of known references to any published

materials describing or analyzing the security of the submitted algorithm. Submission of copies of these materials (accompanied by a waiver of copyright or permission from the copyright holder for AES public evaluation purposes) is encouraged.

2.B.6 A statement shall be included that lists *and describes* advantages and limitations of the algorithm. Such advantages and limitations shall address the ability to:

a. implement the algorithm as a stream cipher, Message Authentication Code (MAC) generator, pseudo-random number generator, hashing algorithm, etc.

b. implement the algorithm in various environments, including—but not limited to: 8-bit processors (smartcards), ATM, HDTV, B–ISDN, voice applications, satellite applications, etc. To demonstrate the efficiency of a hardware implementation of the algorithm, the submitter may include a specification of the algorithm in a nonproprietary Hardware Description Language (HDL).

c. use the algorithm with key- and block-sizes other than those required as a minimum in the Minimum Acceptability Requirements section of this announcement.

If the submitter believes that the algorithm has certain features deemed advantageous by the submitter, then these should be listed and described, along with supporting rationale. Some examples of these features might include, for example: throw-away tables, mathematically (rather than empirically) designed tables, statistical basis for inter-round mixing, variable key setup time, etc.

2.C Magnetic Media

2.C.1 Reference Implementation

A reference implementation shall be submitted, in order to promote the understanding of how the candidate algorithm may be implemented. This implementation shall consist of source code written in ANSI C; appropriate comments should be included in the code, and it should clearly map to the algorithm description included under section 2.B.1. Since this implementation is intended for reference purposes, *clarity in programming* is more important than efficiency.

The reference implementation shall be capable of fully demonstrating the operation of the candidate algorithm. The reference implementation shall support all key- and block-size combinations specified in the Minimum Acceptability Requirements section of this announcement. Additionally, it *must* support all other key-block sizes that are claimed to be supported by the algorithm.

NIST will specify a cryptographic API for the ANSI C implementations, which will be made available at <http://csrc.nist.gov/encryption/aes>. All ANSI C submissions shall implement that API, so that the NIST test system can be compatible with all submissions.

Separate source code for implementing the required Known Answer Tests and Modes Tests with the reference implementation shall also be included. This code shall be able to process input specified in the format indicated by NIST (on the WWW site as referred to under section 2.B.3) and run the required tests.

The reference implementation shall be provided on a single diskette, which shall be labeled with the submitter's name, the algorithm name, and ''Reference Implementation.''

2.C.2 Mathematically Optimized Implementation

Two *mathematically* optimized implementations of the candidate algorithm shall be submitted, so that NIST can perform tests in two different languages in order to demonstrate the potential for efficient implementation. These two implementations shall be specified in ANSI C and Java programming languages:

i. *ANSI C*: The first mathematically optimized implementation shall be specified in ANSI C source code. NIST intends to use the ANSI C compiler specified under ''Round 1 Technical Analysis'' to compile the code and link it to the NIST test system. (NIST received many comments that the optimized implementation should be written in C, since it is a very common language.)

NIST will specify a cryptographic API for the ANSI C implementations, which will be made available at <http://csrc.nist.gov/encryption/aes>. All ANSI C submissions shall implement that API, so that the NIST test system can be compatible with all submissions.

ii. *Java language specification:* The second mathematically optimized implementation shall be specified in the Java programming language, as defined by the Java Development Kit (JDK) version 1.1. This JDK 1.1 is publicly available for multiple platforms from Javasoft, at <http://www.javasoft.com>. NIST has selected Java as one language for the mathematically optimized implementations because it will provide an accurate *relative* mathematical efficiency measure of the different candidate algorithms, since it uses machine-independent code. The use of one Java Virtual Machine—to test all of the Java implementations submitted to NIST—is intended to eliminate differences in hardware optimizations that may occur when using other languages. It is *not* intended that the Java implementation will provide an absolute efficiency measure of each candidate algorithm on the NIST Analysis Platform.

Submissions are required to use the cryptographic API defined by the Java Cryptography Architecture (JCA) in conjunction with the Java Cryptography Extension (JCE). An AES submitter shall create a Cryptography Package Provider (CPP) that implements the submitted candidate algorithm. The Provider class is described in the JCA (Refer to <http://java.sun.com:80/products/jdk/1.1/docs/guide/security/CryptoSpec.html>, under ''The Provider Class''; JCE 1.1 APIs may be found at <http://java.sun.com/security>). The ''Cipher'' engine subclass within the CPP (as defined in the JCE) shall then be used to implement the candidate encryption algorithm. Other appropriate engine subclasses from the JCA and JCE may also be implemented, to accommodate features of the particular candidate algorithm (e.g., ''Key Generator'' class in the JCE).

General Requirements for Both Mathematically Optimized Implementations

Both of the mathematically optimized implementations shall support key- and block-size combinations specified in the Minimum Acceptability Requirements section of this announcement.

The mathematically optimized implementations shall operate in the Electronic Codebook (ECB), Cipher Block Chaining (CBC), and 1-bit Cipher Feedback (1–CFB) modes for encryption and decryption. Other modes are not required to be implemented in the software provided to NIST.

Separate source code for implementing the required Known Answer Tests and Modes Tests with the mathematically optimized implementations shall also be included. This code shall be able to process input specified in the format indicated by NIST (on the WWW site as referred to under section 2.B.3) and run the required tests.

The submitter shall provide the mathematically optimized implementations on two separate diskettes, which shall be labeled with the submitter's name, the algorithm name, and ''Optimized—ANSI C'' or ''Optimized—Java''.

Additionally, submitters may, at their discretion, submit revised optimized

implementations (for both the ANSI C and Java implementations) for use in the Round 2 evaluation process, allowing additional time for improvements. These must be received prior to the beginning of the round 2 evaluation; submittors will be notified of the specific deadline as appropriate. Note that the mathematically optimized implementations on file with NIST at the close of the initial submission period will be the ones used in the Round 1 evaluation.

2.C.3 Test Values—Known Answer Tests and Monte Carlo Tests

The files on this diskette shall contain all of the test values required under section 2.B.3 of this announcement. That section includes descriptions of the required tests as well as a list of the values that must be provided. These files may be compressed using PKZIP or GNUZIP to conserve disk space, if necessary.

The required format for the test vectors will be specified by NIST at <http://csrc.nist.gov/encryption/aes>

The test values shall be provided on a single diskette, which shall be labeled with the submitter's name, the algorithm name, and ''Test Values: Known Answer Tests and Monte Carlo Tests.''

2.C.4 Supporting Documentation

So as to facilitate electronic distribution of submissions to all interested parties, copies of all written materials must also be submitted in electronic form in either PostScript or Adobe PDF. PDF is preferable. (NIST will convert PostScript submissions to PDF.) Submitters planning to create PDF are encouraged to use the thumbnail and bookmark features, to have a clickable table of contents (if applicable), and to include other links within the PDF as appropriate. To create a PostScript file, users of PC word processors should configure their software to print using a PostScript printer driver, and capture the output using the ''print to file'' feature, preferably using standard PostScript printer fonts (not downloaded fonts).

Users of TeX, LaTeX/DVIPS should use PostScript Type 1 fonts, preferably standard PostScript printer fonts, rather than the default embedded bitmapped Computer Modern fonts. Instructions for configuring DVIPS can be found at <http://www.adobe.com/supportservice/custsupport/SOLUTIONS/385e.htm>, ''Creating quality Adobe PDF files from TeX with DVIPS,'' by Kendall Whitehouse/EMERGE, FaxYI number 131303. (This is cited for reference purposes only, and does not constitute a direct or implied endorsement.)

NIST then intends to make submissions available electronically (consistent with U.S. export regulations) in both PostScript and PDF formats.

This electronic version of the supporting documentation shall be provided on diskette(s), which shall be labeled with the submitter's name, the algorithm name, and ''Supporting Documentation.'' If multiple diskettes are necessary, each diskette must also be labeled with ''#*m* of *n*'' as appropriate.

2.C.5 General Requirements for Magnetic Media

A separate diskette shall be used for the reference implementation, mathematically optimized implementations, test values, and supporting materials.

All magnetic media presented to NIST shall be free of viruses or other malicious code. Media submitted will be scanned for the presence of such code. If such malicious code is found, NIST will notify the submitter and ask that a clean version of the magnetic media be re-submitted.

All magnetic media shall be submitted on 3.5″ 1.44MB floppy diskettes, formatted for use on an IBM-compatible PC.

A file labeled ''README'' shall be included on each diskette, listing all files included on the diskette, with a brief description of each.

NIST is in the process of defining a selected set of cryptographic service calls for the ANSI C implementations. For the Java implementation, NIST will use calls from the Java Cryptography Architecture API. These two sets of calls shall be used by the NIST test software to make appropriate calls to the optimized and reference implementations, so that the test software does not have to be rewritten for each submitted algorithm. Therefore, *both the mathematically optimized and reference implementations are required to conform with these specific calls.* The implementations shall be supplied in source code so that NIST can compile and link them appropriately with the test software. The two selected sets of required calls will be available at the following location: <http://csrc.nist.gov/encryption/aes>. NIST intends that these will be available within three months after publication of this notice.

2.D Intellectual Property Statements/Agreements/Disclosures

After review of the public comments on the draft minimum acceptability requirements and evaluation criteria (published for comment in the Federal Register on January 2, 1997), NIST has determined that potential users of the AES desire to have the AES available worldwide on a royalty free basis. Additionally, based upon the results of the April 15, 1997 public workshop held on the draft evaluation criteria and submission requirements, NIST believes there is a reasonable basis to expect a sufficient number and variety of submissions willing to meet these licensing conditions such that the expressed needs of potential AES users can be accommodated.

In order to ensure this and minimize any intellectual property issues, the following statement is required:

2.D.1 Statement by the Submitter

I, _____ (print submitter's full name) _____ do hereby declare that to the best of my knowledge the practice of the algorithm, reference implementation, and mathematically optimized implementations, I have submitted, known as _____ (print name of algorithm) _____ may be covered by the following U.S. and/or foreign patents: _____ (describe and enumerate or state ''none'' if appropriate) _____.

I do herby declare that I am aware of no patent applications which may cover the practice of my submitted algorithm, reference implementation or mathematically optimized implementations. –OR– *I do hereby declare that the following pending patent applications may cover the practice of my submitted algorithm, reference implementation or mathematically optimized implementations:* _____ (*describe and enumerate)* _____.

I do hereby understand that my submitted algorithm may not be selected for inclusion in the Advanced Encryption Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for inclusion in the Federal Information Processing Standard (FIPS) for Advanced Encryption Standard (AES). I further understand that I will not receive financial compensation from the government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications relating to my algorithm. I also understand 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). Should my submission be

selected for inclusion in the AES, I hereby agree not to place any restrictions on the use of the algorithm intending it to be available on a worldwide, non-exclusive, royalty-free basis.

I do hereby agree to provide the statements required by sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover practice of my algorithm, reference implementation or mathematically optimized implementations and the right to use such implementation for the purposes of the AES evaluation process.

I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived 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 implementation, revert back to the submitter (and other owner[s] as appropriate). Additionally, should the U.S. Government not select my algorithm for inclusion in the AES after a period of four years from the close of the submission date for candidate algorithms, all rights revert to the submitter (and other owner[s] as appropriate).

Signed:
Title:
Dated:
Place:

2.D.2 Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner of the patent and patent applications above identified.

I, _____ (print full name) _____, of _____ (print full postal address) _____, am the owner or authorized representative of the owner (print full name, _____ if different than _____ the signer) of the following patent(s) and or _____ patent application(s): _____ (enumerate) _____, and do hereby agree to grant to _____ any interested party if the algorithm known as _____ (print name of algorithm _____, is selected for inclusion in the Advanced Encryption Standard, an irrevocable nonexclusive royalty-free license to practice the referenced algorithm, reference implementation or the mathematically optimized implementations. Furthermore, I agree to grant the same rights in any other patent granted to me or my company which may be necessary for the practice of the referenced algorithm, reference implementation, or the mathematically optimized implementations.

Signed:
Title:
Dated:
Place:

Note that the government may conduct research as may be appropriate to verify the availability of the submission of a royalty free basis worldwide.

2.D.3 Statement by Reference/ Mathematically Optimized Implementations' Owner(s)

The following must also be included:

I, _____ (print full name) _____, am the owner of the submitted reference implementation and mathematically optimized implementations and hereby grant the Government and any interested party the right to use such implementations for the purposes of the AES evaluation process notwithstanding that the implementations may be copyrighted.

Signed:
Title:
Dated:
Place:

2.E General Submission Requirements

NIST welcomes both domestic and international submissions; however, in order to facilitate analysis and evaluation, it is required that the submission packages be in English. This information includes the cover sheet, algorithm specification and supporting documentation, source code, and intellectual property information. Any required information that is submitted in a language other than English shall render the submission package ''incomplete.'' Optional supporting materials (e.g., journal articles) in another language may be submitted.

Classified and/or proprietary submissions shall not be accepted.

3. Minimum Acceptability Requirements

Those packages which are deemed to be ''complete'' will then be evaluated to see if they contain a ''proper'' candidate algorithm. To be considered as a ''proper'' candidate algorithm submissions (and continue further in the AES Development Process), candidate algorithms must meet the following minimum acceptability requirements:

1. The algorithm must implement symmetric (secret) key cryptography.

2. The algorithm must be a block cipher.

3. The candidate algorithm shall be capable of supporting key-block combinations with sizes of 128–128, 192–128, and 256–128 bits. A submitted algorithm may support other key-block sizes and combinations, and such features will be taken into consideration during analysis and evaluation.

(End of minimum acceptability requirements)

Candidate algorithm submission packages which are complete (as defined earlier) and whose algorithm meets the minimum acceptability requirements (as defined immediately above) will be deemed to be ''complete and proper'' submissions. Those deemed otherwise will receive no further consideration. A complete list of submissions will be publicly announced by NIST—those which are ''complete and proper,'' and any others.

4. Evaluation Criteria

In order to provide a basis for the analysis and evaluation of encryption algorithms submitted to be considered for incorporation into the FIPS for AES, evaluation criteria will be used to review candidate algorithms. All of NIST's analysis results will be made publicly available.

Although NIST will be performing its own analyses of the candidate algorithms, NIST strongly encourages public evaluation, making those results publicly available and submitting them to NIST. This information may be addressed at the Second and Third AES Candidate Conferences. NIST will take into account its own analysis, as well as all other input received, in order to make its decision regarding the AES selection.

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 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 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 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.

5. Initial Planning for the First AES Candidate Conference

An open public conference is being planned for the summer of 1998, at which the submitter of each complete and proper nomination package is invited to publicly discuss and explain their candidate algorithm.

Written portions of all submitted candidates will be made available at the Conference, including those not deemed ''complete and proper.'' Submitters of complete and proper submissions will be invited to speak to discuss their submission and answer questions.

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

6. Plans for Candidate Evaluation Process

This section provides an overview of the envisioned AES candidate review process, including NIST's plans for technical analysis of submissions.

6.A Overview

Following the close of the call for candidate algorithm submission packages, NIST will review them to determine which are ''complete and proper,'' as described elsewhere in this notice. NIST then intends to make all submissions publicly available (consistent with U.S. export regulations) and invite public comments on the ''complete and proper'' submissions. To help better inform the public, the First AES Candidate Conference will be held at the start of the public comment process to allow submitters to publicly explain and answer questions regarding their submissions. NIST intends to publish a separate **Federal Register** notice in the future requesting public comments on the candidate algorithms in the Round 1 evaluation to be used in narrowing of the candidate pool for more careful study and analysis in Round 2.

During the Round 1 public review, NIST intends to technically evaluate the candidate algorithm as outlined in the ''Round 1 Technical Evaluation'' section below. Note that NIST does not intend to conduct its own cryptanalysis, but, rather it will review the public evaluations of the candidate algorithms' cryptographic strengths and weaknesses, and NIST will use these in determining if an algorithm meets the objectives of the AES. Because of limited resources, and also to avoid moving evaluation targets (i.e., modifying the submitted algorithms undergoing public review), NIST will not accept modifications to the submitted algorithm during Round 1.

For informational and planning purposes, near the end of the Round 1 public evaluation process, NIST intends to hold the Second AES Candidate Conference (approximately six months after the first conference; exact date to be scheduled.) Its purpose will be to publicly discuss the AEA candidate algorithms by NIST and others, and provide NIST with advice for narrowing the field of algorithms to be considered for the AEA.

NIST thereafter intends to narrow the field of candidates to no more than five candidate algorithms based upon its own analysis, public comment, and all other available information. It is envisioned that this narrowing will be done primarily on security, efficiency, and intellectual property considerations.

Before the start of Round 2 evaluation, submitters have the option of providing updated mathematically optimized implementations for use during the second phase of evaluation (for those algorithms remaining in the Round 2 evaluation). During the course of Round 1 evaluations it is conceivable that some small deficiencies may be identified in even some of the most promising

candidates. Therefore, for the Round 2 evaluations, small modifications to the submitted algorithms will be permitted for their security or efficiency purposes. Submitters may submit minor changes (no substantial redesigns) along with a supporting explanation/justification (see below) which must be received by NIST prior to the beginning of Round 2. (Submitters will be notified by NIST of the exact deadline.) If this option is exercised, new reference and mathematically optimized implementations and written descriptions must also be provided by the start of Round 2. This will allow public review of the modified algorithms during the entire course of the second evaluation.

Note: All proposed changes for Round 2 must be proposed by the submitter; no proposed changes (to the algorithm or implementations) will be accepted from a third party.

After the narrowed list of candidate algorithms is officially announced, NIST intends that a six to nine month public review period will follow (the Round 2 evaluation). During the public review, NIST intends to technically evaluate the candidate algorithms as outlined in the two sections below. Near the end of the public review period, NIST intends to hold the Third AES Candidate Conference. (The exact date is to be scheduled.)

NIST then will select the algorithm(s) for inclusion in the AES, which will be incorporated into a draft FIPS, which NIST intends to announce in the **Federal Register** for comment.

Note that this schedule for the AES development is somewhat tentative, depending in part upon the type, quantity, and quality of submissions. Specific conference dates and public comment periods will be announced at appropriate times in the future. Note also that as a result of comments received on the draft evaluation criteria and submission requirements, NIST has further extended the length of time for algorithm submissions and each of the ensuing planned public comment periods.

6.B Round 1 Technical Evaluation

NIST will invite public comments on all complete and proper submissions. NIST's Round 1 analysis are intended, at a minimum, to be performed as follows:

i. Key-Block Size Combinations: Round 1 testing by NIST will be performed on the 128-bit key and 128-bit block size combination. (The public, however, is welcome to also focus on other key- and block-size combinations.) Testing of other key-block sizes may be accomplished if time and resources permit.

ii. Correctness check: The Known Answer Test and Monte Carlo Test values included with the submission will be used to test the correctness of the reference and mathematically optimized implementations, once they are compiled. *(It is more likely that NIST will perform this check of the reference code—and possibly the optimized code as well—even before accepting the submission package as ''complete and proper.'')*

iii. Efficiency testing: Using the submitted mathematically optimized implementations, NIST intends to perform various computational efficiency tests for the 128–128 key-block combination, including the calculation of the time required to perform:

—Algorithm setup,
—Key setup,
—Key change, and
—Encryption and decryption.

NIST may perform efficiency testing on other platforms.

iv. Other testing: Other features of the candidate algorithms may be examined by NIST.

Platform and Compilers

The above tests will be performed by NIST with the following tools, at a minimum. Due to limited resources, NIST has limited its own efficiency analysis to a single, common platform; however, NIST invites the public to conduct similar tests and compare results on additional platforms (e.g., RISC processors, 8-bit processors, Digital Signal Processors, dedicated CMOS, etc.).

i. NIST Analysis Platform: IBM-compatible PC, with an Intel Pentium Pro Processor, 200MHz clock speed, 64MB RAM, running Windows95.

ii. Compiler (Note that the selection of these two compilers is for use by NIST in the Rounds 1 and 2, and does not constitute a direct or implied endorsement by NIST.):

(a) For the *reference* implementation, NIST intends to use the ANSI C compiler in the Borland C++ Development Suite 5.0.

(b) For the *mathematically optimized* implementations, NIST intends to use the following compilers:

(1) *ANSI C implementation:* ANSI C compiler found in the Borland C++ Development Suite 5.0, and

(2) *Java implementation:* NIST intends to use the bytecode compiler and virtual machine provided in Javasoft's Java Development Kit (JDK) 1.1.

Note: any changes to the intended platform/compiler will be noted on <http://csrc.nist.gov/encryption/aes>.

6.C Round 2 Technical Evaluation

At the end of the Round 1 Technical evaluation and the Second AES Candidate Conference, NIST intends to narrow the field of candidate algorithms to five or fewer, in order to focus the remaining efforts of both NIST and the public. Once again, NIST intends to perform its own analysis of the submissions, and make that information publicly available. NIST's Round 2 analysis will, at a minimum, be performed as follows. *Note: the same platform and compilers from Round 1 will be used for the Round 2.*

i. Key-Block Size Combinations: Round 2 testing by NIST will be performed on the minimum key-block combinations specified in the Minimum Acceptability Requirements (beyond the 128-128 key-block combination that was evaluated in Round 1). *Note: If the submitter chose to submit updated mathematically optimized implementations prior to the beginning of Round 2, then some of the tests performed in Round 1 for the 128-128 combination may be performed again using the new mathematically optimized implementations. This will be done to obtain updated measurements.*

ii. Efficiency testing: Using the submitted mathematically optimized implementations, NIST intends to perform various computational efficiency tests for the minimum key-block combinations specified in the Minimum Acceptability Requirements, including the calculation of the time required to perform:

—Algorithm setup,
—Key setup,
—Key change, and
—Encryption and decryption.

NIST will welcome comments regarding the efficiency of the candidate algorithms when implemented in hardware. NIST may pursue having the remaining algorithms specified using a Hardware Description Language, to compare the estimated hardware efficiency of the candidate algorithms.

NIST may perform efficiency testing using additional platforms. Once again, NIST welcomes public input regarding efficiency testing on additional platforms.

iii. Other testing: Other features of the candidate algorithms may be examined by NIST. If appropriate, analyses from the Second AES Candidate Conference and the public evaluation during Round 1 may warrant the testing of specific features.

7. Miscellaneous

This section is intended to address some of the questions/comments raised in the review of the draft evaluation criteria.

When evaluating algorithms, NIST will make every effort to obtain public input and will encourage review of the candidate algorithms by outside organizations; however, the final decision as to which algorithms(s) will be proposed to the Secretary of Commerce for inclusion in the AES is the responsibility of NIST.

NIST intends to develop a validation program for AES conformance testing, with the goal of having it operational concurrently with the effective date of the AES.

NIST does NOT have a fixed timeable for completion of the AES.

NIST is not specifically seeking a stream cipher algorithm, since any block cipher algorithm can be operated in a stream cipher mode.

NIST does not intend to select a wholly distinct algorithm for each of the minimum required key-block combinations. It is strongly recommended that no submission be so constructed.

NIST does not wish to target a specific application or platform for implementing the AES, as the evaluation of candidate algorithms takes place. However, one factor that is being taken into consideration for each candidate algorithm is its flexibility—the ability to implement the algorithm securely and efficiently in a wide variety of platforms and applications (see ''Algorithm and Implementation Characteristics'' under ''Evaluation Criteria'' section).

NIST does not intend to select a ''backup'' AES algorithm. Rather, should the circumstances arise (e.g., discovery of a significant security flaw) which could not be satisfactorily addressed by modifying the AES, NIST would likely look to the other AES candidate finalists. Additionally, if a significant period of time has elapsed since the AES selection, it would also make sense to examine other algorithms which may have been developed in the intervening period.

Exportability decisions regarding submissions and, eventually, products implementing AES will be made by the appropriate government regulatory authorities. NIST is a non-regulatory agency of the U.S. Department of Commerce.

NIST does not intend to offer financial incentives (e.g., contests) for cryptanalysis of AES candidates.

Should no appropriate algorithms be submitted in response to this call, NIST expressly reserves the right to cease this process and examine other possible courses of action.

Submitters are strongly encouraged to submit only one algorithm each (presumably the one in which the submitter has the greatest confidence). Submission of similar, yet distinct, algorithms may delay the public evaluation process and may well raise public questions as to the submitter's level of confidence in his/her candidates.

For conference and resource allocation planning purposes, it would be appreciated if those planning to submit candidates could notify the individuals listed in the ''For Further Information'' section as soon as possible.

Appreciation

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

Dated: September 8, 1997.

Elaine Bunten-Mines,

Director, Program Office.

[FR Doc. 97–24214 Filed 9–11–97; 8:45 am]

BILLING CODE 3510–CN–M

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 080697D]

Request for Nomination of Individuals for the Federal Investment Task Force (Deadline Extension)

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of request for nominations deadline extension.

SUMMARY: The Sustainable Fisheries Act (SFA) requires the Secretary of Commerce (Secretary) to establish a task force to study the role of the Federal Government in subsidizing fleet capacity and influencing capital investment in fisheries. NMFS is extending the deadline for nominations of qualified individuals to serve on the task force.

DATES: Nominations will now be accepted through October 1, 1997.

ADDRESSES: Nominations should be sent to Atlantic States Marine Fisheries Commission, 1444 Eye Street, NW, 6th Floor, Washington, DC 20005, ATTN: Federal Investment Task Force. Nominations may be submitted by fax, (202) 289–6051

FOR FURTHER INFORMATION CONTACT: Robert Beal, Atlantic States Marine Fisheries Commission, (202) 289–6400.

SUPPLEMENTARY INFORMATION: The Secretary is establishing a task force of interested parties to study the role of the Federal Government in (1) subsidizing the expansion and contraction of fishing capacity in fishing fleets the Magnuson-Stevens Fishery Conservation and Management Act, and (2) otherwise influencing the aggregate capital investment in fisheries. The original request for nominations was published in the **Federal Register** at Vol. 62, No. 167/Thursday August 28, 1997, page 45628. However, in order to allow sufficient time for all interested parties to submit nominations, the deadline for submission has been extended through October 1, 1997. The procedures and guidelines for submitting nominations can be found in the original **Federal Register** notice.

Please note: The task force is now tentatively scheduled to meet five times between November 1997 and June 1997.

Dated: September 8, 1997.

David L. Evans,

Deputy Assistant Administrator for Fisheries, National Marine Fisheries Service.

[FR Doc. 97–24263 Filed 9–9–97; 3:19 pm]

BILLING CODE 3510–22–F

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

[I.D. 090497A]

Spiny Dogfish in U.S. Waters in the Western Atlantic Ocean; Scoping Process

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of intent to prepare an environmental impact statement (EIS) and request for scoping comments.

SUMMARY: The Mid-Atlantic and New England Fishery Management Councils (Councils) announce their intention to jointly prepare, in cooperation with NMFS, an EIS to assess potential effects on the human environment of a management regime for spiny dogfish (*Squalus acanthias*) pursuant to the Magnuson-Stevens Fishery Conservation and Management Act of 1976, as amended (Magnuson-Stevens Act). This would be accomplished through the development of a Spiny Dogfish Fishery Management Plan (FMP). If such an FMP is approved by the Secretary of Commerce (Secretary),