Billing Code: 3510-CN

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

(Docket No. 000929280-1201-02

RIN No. 0693-ZA42

Announcing Approval of Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES)

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

ACTION: Notice.

SUMMARY: The Secretary of Commerce approves FIPS 197, Advanced Encryption Standard (AES), and makes it compulsory and binding on Federal agencies for the protection of sensitive, unclassified information. A new robust encryption algorithm was needed to replace the aging Data Encryption Standard (FIPS 46-3), which had been developed in the 1970s. In September 1997, NIST issued a Federal Register notice soliciting an unclassified, publicly disclosed encryption algorithm that would be available royalty-free worldwide. Following the submission of 15 candidate algorithms and three publicly held conferences to discuss and analyze the candidates, the field was narrowed to five candidates. NIST continued to study all available information and

analyses about the candidate algorithms, and selected one of the algorithms, the Rijndael algorithm, to propose for the AES.

EFFECTIVE DATE: This standard is effective May 26, 2002.

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

A copy of FIPS 197 is available electronically from the NIST website at: <http://csrc.nist.gov/encryption/aes/index.html />.

SUPPLEMENTARY INFORMATION: A notice was published in the Federal Register (Volume 66, Number 40, pp. 12762-3) on February 28, 2001, announcing the proposed FIPS for Advanced Encryption Standard for public review and comment. The Federal Register notice solicited comments from the public, academic and research communities, manufacturers, voluntary standards organizations, and Federal, state, and local government organizations. In addition to be published in the Federal Register, the notice was posted on the NIST Web pages; information was provided about the submission of electronic comments. Comments and responses were received from 21 private sector organizations, individuals, and groups of individuals, and from one federal government organization. None of the comments opposed the adoption of the AES as a Federal Information Processing Standard. Comments supported the

selection of the algorithm and commended the clear, well-written presentation of the standard. Some comments offered editorial suggestions, pointed out perceived inconsistencies in the text, and requested clarifications. All of the editorial recommendations were carefully reviewed, and changes were made to the standard where appropriate.

Following is an analysis of the technical and related comments received.

Comment: The FIPS for AES should include support for additional block and key sizes. This would take advantage of the AES algorithm's built-in flexibility, making it better suited for use in a hashing mode and with communications applications that require minimal overhead (padding).

Response: NIST recognizes that one of the AES algorithm's strengths is its inherent support for additional block and key sizes. However, other block and key sizes have not been subjected to the same public analyses as those sizes that are provided for in the recommended FIPS. As a result, NIST believes that it would not be appropriate to include the additional sizes at this time. The block and key sizes are specified as parameters in the recommended FIPS, and could be modified to include other block and key sizes in the future if needed. The recommended standard explains that the use of parameters in the specification is intended to encourage AES implementers to build their applications and systems with future flexibility and adaptability in mind. NIST will monitor future developments, and will consider adding more parameters to the specification if needed in the future.

Comment: For added security, and to meet the needs for extremely long-term security, NIST should increase the number of rounds that are specified by the AES algorithm (i.e., the amount of processing used for encryption and decryption). Since new techniques to break the algorithm may evolve, the margin of security offered by the algorithm should be increased.

Response: Prior to its evaluation of the five finalist candidate algorithms, NIST's AES selection team discussed the issue of whether the number of rounds should be changed for one or more of the algorithms; the selection team decided to consider only the algorithms as initially submitted. Changing the number of prescribed rounds would change the way that the algorithm was defined (e.g., its key schedule), and the process of proposing, reviewing, and evaluating an algorithm would have to start over from the beginning. If the number of rounds were changed, many of the security and performance analyses that had already been performed on the candidate algorithms would no longer be useful.

Furthermore, throughout the development and review of the recommended FIPS, there was little agreement on which key sizes should have more rounds, and less agreement on how many rounds to add. Some who commented on the Draft FIPS proposed adding just two rounds, while another comment suggested adding 114 rounds.

NIST is not aware of advances in cryptographic techniques that would threaten the security provided by the recommended FIPS, but will continue to follow developments, to reevaluate the

standard, and to consider changes or additions that might be needed. As with its other cryptographic standards, NIST will review the recommended FIPS every five years to consider whether the standard should be reaffirmed, amended, or withdrawn.

Comment: Since the AES algorithm allows three different key sizes, NIST should provide guidance to users regarding how and for what purpose(s) the different keys should be used.

Response: NIST is currently developing a guideline that will address numerous key management issues, including considerations for selecting from among multiple key sizes. Details on the content and development of that guideline are available on NIST's web pages http://csrc.nist.gov/encryption/kms/white-paper.pdf.

Comment: Statements in the FIPS are unclear and ambiguous regarding validation requirements for AES implementations. Additionally, many of these statements refer to FIPS 140-2, which has not been approved and which has a transition period when both FIPS 140-1 and FIPS 140-2 are in effect.

Response: FIPS 140-2 was approved in May 2001, and became effective on November 25, 2001. However, references to FIPS 140-2 have been removed in order to limit any misunderstandings.

Following approval of this recommended FIPS, vendors may request that their AES implementation be tested and validated either for conformance to the AES specification or in conjunction with a cryptographic module validation test (i.e., validation testing for FIPS 140-2). The process is the same for all testing of implementations of FIPS-approved algorithms under the Cryptographic Module Validation Program.

Comment: Comments indicated concern about the padding to be used when the length of the data to be encrypted was not an even multiple of the block size. Other comments proposed more optimal specifications of the algorithm.

Response: NIST considers padding and optimization to be outside the scope of this standard. Padding will be addressed in a standard or recommendation to be developed on the modes of operation for the AES, and in the applications and protocols that use the AES.

It is expected that many optimizations of the AES will be developed over time. NIST plans to post information that it receives on optimization issues on its web pages with the permission of the submitter.

Comment: One comment recommended the selection of a different algorithm, one that had not been submitted during the AES development process.

Response: NIST conducted an open process to solicit and evaluate algorithms for consideration for the AES. All candidate algorithms have been thoroughly reviewed and analyzed by the international cryptographic community.

AUTHORITY: Under Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to approve standards and guidelines for the cost effective security and privacy of sensitive information processed by federal computer systems.

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

Dated:

Karen H. Brown
Acting Director, NIST