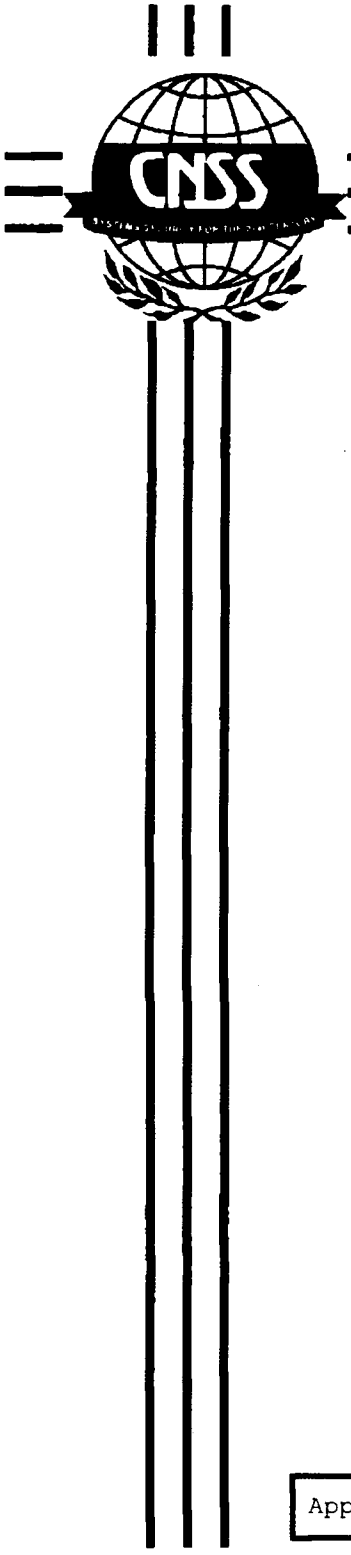

CNSS Policy No. 15
February 2003

NATIONAL POLICY
ON
THE USE OF THE
ADVANCED ENCRYPTION STANDARD (AES)
TO PROTECT
NATIONAL SECURITY SYSTEMS AND
NATIONAL SECURITY INFORMATION

This document prescribes minimum standards. Your department or agency may require further implementation.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Committee on National Security Systems

CNSS Policy No. 15

CHAIR

1. (U) Federal Information Processing Standard (FIPS) No. 197, dated 26 November 2001, promulgated and endorsed the Advanced Encryption Standard (AES) as the approved algorithm for protecting sensitive (unclassified) electronic data. Since that time, questions have arisen whether AES (or products in which AES is implemented) can or should be used to protect classified information and at what levels. Responsive to those questions, the National Security Agency (NSA) has conducted a review and analysis of AES and its applicability to the protection of national security systems and/or information. The policy guidance documented herein reflects the results of those efforts.

2. (U) The issuance of this policy is reflective of the Committee's desire to remain responsive to the changing Information Assurance (IA) needs of the nation, and is consistent with the future direction for the Committee as documented in NSTISSC-034-99, Subject: Information Assurance Position Paper, dated 26 April 1999.

3. (U) CNSS Representatives may obtain additional copies of this policy from the address below. U.S. Government contractors should contact their appropriate government Contracting Office Representative (COR) regarding further distribution and dissemination of this document.

John P. Stenbit

(b) (6)

CNSS Secretariat [redacted]. National Security Agency . 9800 Savage Road STE 6716 . Ft Meade MD 20755-6716

[redacted]

(b) (3)-P.L. 86-36

CNSS Policy No. 15

(U) NATIONAL POLICY ON THE USE OF THE ADVANCED ENCRYPTION STANDARD (AES) TO PROTECT NATIONAL SECURITY SYSTEMS AND NATIONAL SECURITY INFORMATION

SECTION I - (U) SCOPE

1. (U) This policy is applicable to all U.S. Government Departments or Agencies that are considering the acquisition or use of products incorporating the Advanced Encryption Standard (AES) to satisfy Information Assurance (IA) requirements associated with the protection of national security systems and/or national security information.

SECTION II - (U) BACKGROUND

2. (U//~~FOUO~~)

a.

b.

c.

d.

3. (U) The above realities dictate the adoption of a flexible and adaptable strategy that encourages the use of a mix of appropriately implemented NSA-developed algorithms, and those available within the public domain. The policy set forth below reflects those realities and the strategy.

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

SECTION III - (U) POLICY

4. (U//~~FOUO~~)

5. (U//~~FOUO~~)

6. (U) Subject to policy and guidance for non-national security systems and information (e.g., FIPS 140-2), U.S. Government Departments and Agencies may wish to consider the use of security products that implement AES for IA applications where the protection of systems or information, although not classified, nevertheless, may be critical to the conduct of organizational missions. This would include critical infrastructure protection and homeland security activities as addressed in Executive Order 13231, Subject: Critical Infrastructure Protection in the Information Age (dated 16 October 2001), and Executive Order 13228, Subject: Homeland Security (dated 8 October 2001), respectively. Evaluations of products employing AES for these types of applications are subject to review and approval by the National Institute of Standards and Technology (NIST) in accordance with the requirements of Federal Information Processing Standard (FIPS) 140-2.

(b)(3)-18 USC 798
(b)(3)-P.L. 86-36

[1] (U//~~FOUO~~)

SECTION IV – (U) RESPONSIBILITIES

7. (U) U.S. Government Departments or Agencies desiring to use security products implementing AES to protect national security systems and/or information, or other mission critical information related to national security, should submit the details of their requirements to the Director, National Security Agency (ATTN: IA Directorate, V1) for review. NSA will employ established programs (e.g., NSA sponsored developments, the Commercial COMSEC Endorsement Program (CCEP), or the User Partnership Program) in developing and certifying AES security products for these requirements.

8. (U) The Director, National Security Agency shall:

a. (U) Review and approve all cryptographic implementations intended to protect national security systems and/or national security information.

b. (U) Provide advice and assistance to U.S. Government Departments and Agencies in identifying protection requirements and selecting the encryption algorithms and product implementations most appropriate to their needs.

9. (U) The Director, National Institute and Standards (NIST) shall provide advice and assistance to U.S. Government Departments and Agencies regarding the use of AES for protecting sensitive (unclassified) electronic data.

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

DISTRIBUTION:

[redacted]

(b)(3)-P.L. 86-36