FACT SHEET

CNSS Policy No. 15, Fact Sheet No. 1
National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information

June 2003

Background

(1) 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.

Introduction

(2) In the context of today's complex world and even more complex communicating environments, the need for protecting information takes on added importance and significance. The protection of information is not solely dependent on the mathematical strength of an algorithm that may be a part of a communications security device or a communications system, nor is the selection of that algorithm based only on the classification of the information to be protected. Many factors come into play in deciding what algorithm can or should be used to satisfy a particular requirement. These include:

- The quality of implementation of the algorithm in specific software, firmware, or hardware

- Operational requirements associated with U.S. Government-approved key and key management activities;

- The uniqueness of the classified information to be protected; and/or

- Requirements for interoperability both domestically and internationally.

(3) 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.

Scope

(4) 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.

Policy

(5) NSA-approved cryptography[1] is required to protect (i.e., to provide confidentiality, authentication, non-repudiation, integrity, or to ensure system availability) national security systems and national security information at all classification levels.

(6) The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.

(7) 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.

[1] NSA-approved cryptography consists of an approved algorithm; an implementation that has been approved for the protection of classified information in a particular environment; and a supporting key management infrastructure.

Responsibilities

(8) 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.

(9) The Director, National Security Agency shall:

- Review and approve all cryptographic implementations intended to protect national security systems and/or national security information.

- 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.

(10) 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.