CNSS Advisory Memorandum
Information Assurance/03-04
November 2004

(U) Advisory Memorandum for Information Assurance (IA) – Advanced Encryption Standard (AES) Implementation

CNSS Advisory Memorandum
Information Assurance/03-04

Committee on National Security Systems

## National Manager

(U) FOREWORD

1. (U) This memorandum clarifies CNSS Policy Number 15 on the Advanced Encryption Standard (AES) and provides guidance necessary for its implementation within U.S. Government departments and agencies.

2. (U) Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this memorandum from the Secretariat at the address listed below.

3. (U) I encourage dissemination of the contents of this memorandum to all Government entities, vendors, and contractors engaged in IA activities associated with national security systems.

/s/
MICHAEL V. HAYDEN
Lieutenant General, USAF

CNSS Secretariat [redacted] National Security Agency. 9800 Savage Road . STE 6716Ft. Meade, MD 20755-2716
[redacted]

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

CNSS Advisory Memorandum
Information Assurance/03-04

(U) Advisory Memorandum
Information Assurance (IA) –
Advanced Encryption Standard (AES) Implementation

1. (U) Purpose – CNSS Policy Number 15, "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information," dated February 2003, states that "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." Further, the policy also states "NSA will employ established programs in developing and certifying AES security products." The following clarifies that policy.

2. (U) Selection and Use of AES – NSA has existing programs in place to assist government organizations and vendors in the development and certification of products for national security systems (e.g., NSA certification processes, the Commercial COMSEC Evaluation Program (CCEP), and the User Partnership Program (UPP)). Further, NSA has a key management infrastructure for generating the keying material necessary for enabling the secure operations of certified security products.

3. (U) While the commercial AES cryptographic algorithm has been approved by the government for encrypting national security information, this approval does not imply that products using AES are automatically certified for use in national security systems. Without a full product evaluation, it is impossible to confidently state that products using the AES algorithm are automatically suitable for use in protecting national security information. Any algorithm, even one as sound as AES, can easily be implemented in a very insecure manner. Hence, before approving an AES product for use in a national security system, NSA must first review the implementation of the algorithm and other features of the product using one of its existing programs.

4. (U//~~FOUO~~) [redacted]

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

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

[redacted]

a. (U//~~FOUO~~) [redacted]

b. (U) Vendors planning to use the AES in products intended for the national security market must have a government sponsor for their security product. They should contact the NSA Business Affairs Organization (BAO) at the beginning of the development of the product to reduce the risk of complications associated with certification.

(1) (U) Vendors that have received Federal Information Processing Standard (FIPS) certification for their AES module still require a product sponsor and must contact the NSA BAO to determine if there are any additional certification requirements.

(2) (U) The BAO may be contacted by calling [redacted]

5. (U) After NSA has reviewed a particular AES implementation, it will issue a certification statement defining the operational parameters for the product. This statement demonstrates that a specific product in a specific configuration is suitable for use in protecting national security information.

6. (U) In addition, NSA will ensure the availability of keying material for the certified security product provided an approved product key management plan is in place.

7. (U) Questions regarding which AES products have been NSA certified or the use of AES in future products may be directed to your department or agency COMSEC office, the NSA Information Assurance Business Affairs Organization, or the NSA Business and Customer Relations Office (as above). Questions about AES keying material for NSA certified products should be directed to the NSA Cryptographic Products and Support Center at [redacted]

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

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

DISTRIBUTION:

[redacted]

CNSS Advisory Memorandum
INFOSEC 01-02
March 2002

(U) Advisory Memorandum for Common Terminology Associated with the Electronic Key Management System

This document contains information exempt from mandatory disclosure under the FOIA. Exemption 3 applies.

The information contained herein that is marked U//FOUO is for the exclusive use of the DoD, other U.S. government, and U.S. contractor personnel with a need-to-know. Such information is specifically prohibited from posting on unrestricted bulletin boards or other unlimited access applications, and to an e-mail alias.

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER INFORMATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

CNSS Advisory Memorandum
INFOSEC 01-02

Committee on National Security Systems

National Manager

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

FOREWORD

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

2. (U) This document supersedes Annex D to NSTISSI No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Material, dated August 1997.

3. (U) Representatives of the Committee on National Security Systems (CNSS) may obtain additional copies of this memorandum from the Secretariat at the address listed below.

Michael V. Hayden
MICHAEL V. HAYDEN
Lieutenant General, USAF

CNSS Advisory Memorandum
INFOSEC 01-02

ADVISORY MEMORANDUM
FOR COMMON TERMINOLOGY ASSOCIATED WITH THE
ELECTRONIC KEY MANAGEMENT SYSTEM

1. (U) Purpose and Scope - This Advisory Memorandum describes the Electronic Key Management System (EKMS) architecture, roles and responsibilities of the Key Management Entity (KME), and procedural requirements used for handling and accounting for electronic keys generated and distributed by components of the EKMS. Electronic key will be hereafter referred to as "key."

2. (U) EKMS Architecture - The EKMS is an interoperable collection of systems developed to automate the planning, ordering, generation, distribution, accounting, storage, loading, usage, and destruction of key and the handling and management of other types of physical key and COMSEC material. The EKMS architecture is made up of four hierarchical levels known as Tiers.

a. (U//~~FOUO~~) [redacted]

(1) (U) National COMSEC Material Generation and Production facilities for physical and electronic keys, both traditional and modern.

(2) (U) Central Office of Record (COR) services for NSA, contractor, and select Civil Agency accounts.

(3) (U) National Distribution Authority (NDA) for U.S. accounts worldwide.

(4) (U) National Registration Authority for all non-military accounts on U.S. systems.

(5) (U) National Credential Manager for all EKMS accounts on U.S. systems.

(6) (U) EKMS Defense Courier Service (DCS) data administrator.

b. (U//~~FOUO~~) [redacted]

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

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

[redacted]

1) (U) Common military traditional electronic key generation and distribution facilities.

2) (U) Common key ordering interface for all key types required by military accounts.

3) (U) COR for U.S. military accounts worldwide.

4) (U) Registration Authority for U.S. military accounts. (See paragraph 4.g.)

5) (U) Ordering Privilege Manager for U.S. military accounts. (See paragraph 4.l.)

6) (U) Management for the military's COMSEC Vaults, Depots, and Logistics Systems (VDLS) facilities.

c. (U//~~FOUO~~) [redacted]

(U) NOTE: [redacted]

d. (U//~~FOUO~~) [redacted]

3. (U) EKMS Components

a. (U) Local Management Device (LMD) - Component in EKMS that provides electronic management of key and other COMSEC material and serves as an interface to the Key Processor. (It is composed of a user-supplied personal computer, an operating system, LCMS, and User Application Software (UAS), as required.)

b. (U) Local COMSEC Management Software (LCMS) - Application-level software that provides for the management of key, physical COMSEC materials, non-cryptographic services, and communications. Through a graphical interface, the LCMS automates the functions of the COMSEC Account Custodian/Manager, including accounting, auditing, distribution, ordering, and production. Programs and systems that have specialized key management requirements may choose to develop software shell programs (known as User Application Software or UAS) that run on the LMD with the LCMS software to provide custom functionality.

c. (U) Key Processor (KP) – High-assurance cryptographic component in EKMS designed to provide for the local generation of keying material, encryption and decryption of key, key load into fill devices, and message signature functions.

d. (U//~~FOUO~~) [redacted]

e. (U//~~FOUO~~) [redacted]

f. (U//~~FOUO~~) [redacted]

g. (U//~~FOUO~~) [redacted]

(U) **NOTE:** For specific information on EKMS components, see the System Doctrines.

4. (U) Roles and Responsibilities of Key Management Entities

(U) **NOTE:** These roles and responsibilities vary at activities due to Tier levels and possible manpower constraints. Some elements bear the responsibilities of more than one role.

a. (U) Key Management Entity (KME) - Any activity/organization that performs key management-related functionality and has been assigned an EKMS ID. All IDs are registered by their Registration Authority at the Directory Server.

b. (U) COMSEC Custodian/Manager - Person responsible for the LMD/KP and its operators who handle and account for physical and electronic keys and other COMSEC accountable items.

c. (U) LMD/KP Operator - Person performing routine key management activities on the LMD/KP as authorized by the COMSEC Custodian/Manager. The LMD/KP operator's responsibilities include ordering, generating, distributing, inventorying, and destroying key material.

d. (U) Subaccount - A subaccount receives key only from, and reports only to, its parent account, never a Central Office of Record. It is assigned a unique EKMS ID, may have an LMD or LMD/KP, and may be authorized to receive its key via the Message Server. Subaccounts are Tier 2 elements.

e. (U) Local Element - Shares the EKMS ID of the servicing account or subaccount and can be issued key that will be placed in an ECU or fill device. A fill device may only further load another fill device (e.g., DTD to DTD) with authorization from the COMSEC Custodian/Manager. Local Elements are Tier 3 elements.

f. (U) Privilege Certificate Manager (PCM) - The KME authorized to create the Privilege Certificate for another KME. The EKMS ID of the PCM will be included in the Privilege Certificate and in the PCM field of the associated Message Signature Key (MSK).

g. (U) Registration Authority (RA) - The KME within each Service or Agency responsible for registering KMEs and assigning EKMS IDs to them. Is also responsible for ordering initialization key for KPs and for maintaining registration data on its KMEs in the EKMS Directory Service.

h. (U) Command Authority - The KME responsible for the appointment of User Representatives for a department, agency, or organization and granting of modern (electronic) key ordering privileges for those user representatives.

i. (U) Controlling Authority - The official responsible for directing the operation of a cryptonet and for managing the operational use and control of keying material assigned to the cryptonet. Controlling Authorities are assigned EKMS IDs and are registered KMEs on the Directory Servers, but Controlling Authority is not a notated role on the Directory Server.

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

j. (U//~~FOUO~~) [redacted]

k. (U//~~FOUO~~) [redacted]

l. (U) Ordering Privilege Manager (OPM) - The KME authorized to designate other KMEs as a Short Title Assignment Requester (STAR) or OPM. Authorized to perform STAR functions.

m. (U) Short Title Assignment Requester (STAR) - The KME privileged to request assignment of a new short title and generation of key against that short title. STAR privileges must be registered at the generating account.

n. (U) Authorized ID - The KME authorized to order against a traditional short title. Authorized IDs are associated with each short title. An Authorized ID can also modify the key attributes including the distribution profile for an associated short title. Number of Authorized IDs per short title will be limited to one.

> **NOTE:** Authorized IDs are limited to one unless the Controlling Authority, in coordination with the generating element, approves the additional Authorized IDs.

o. (U//~~FOUO~~) [redacted]

p. (U) Central Office of Record (COR) - The KME that keeps records of accountable COMSEC material held by COMSEC accounts subject to its oversight.

5. (U) Accounting Legend Codes (ALCs) 6/7 and Reg 0 Key - EKMS provides a clear distinction between the handling of hard copy key and electronic key. Refer to paragraphs 60 through 63 in NSTISSI No. 4005, Safeguarding Communications Security (COMSEC) Facilities and Material, dated August 1997, for specific definition of ALC-6 and -7.

a. (U//~~FOUO~~) [redacted]

b. (U//~~FOUO~~) [redacted]

(1) (U) Description of ALC-6 Key and Register Numbers:

(a) (U//~~FOUO~~) [redacted]

(b) (U//~~FOUO~~) [redacted]

(2) (U) Accounting for Reg 0 Key - All Reg 0 key is accountable per its ALC. The method is as follows:

(U) An account is responsible for accounting for one copy of a particular Reg 0. In the event that a Reg 0 key must be copied and distributed, the inventory holdings of the account that is copying and distributing the key will not be decremented. If the receiving account is already in possession of the key when processing an incoming Bulk Encrypted Transaction (BET), the account's inventory holdings are not incremented. However, if the account is not already in possession of the key when a transfer is done, the receiving account's inventory is charged with one copy. Although an account is never accountable for more than one copy of a particular Reg 0 key, the LMD/KP will not mark the key totally destroyed until all copies issued within the account are eliminated.

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

6. (U) Physical Key Conversion to Electronic Form

a. (U) Physical key received and subsequently imported (process by which physical key is converted to electronic key) into a KP will be assigned an electronic short title and an ALC appropriate to electronic key. In electronic form, ALC-1 physical key will be assigned ALC-6 and ALC-4 physical key will be assigned ALC-7.

(U) **NOTE:** FIREFLY key in an LMD/KP is ALC-6, but once it is issued to a physical KSD-64, the key becomes ALC-1.

b. (U) Physical key loaded directly to a DTD will retain its original short title. If the key is subsequently imported into an LMD/KP, it will be handled as stated in paragraph 6a. above.

7. (U) Electronic Key on Physical Media

a. (U) All physical media (floppy disks, magnetic tapes, CD ROMs, optical disks, etc.) that are to be transferred between accounts (other than KSD-64s) on which electronic keys have been loaded will be assigned a short title (or if produced locally, some type of unique identifier and control number) and an ALC of 1 or 4, as directed by the controlling authority (encryption, classification, etc. are factors in the assignment). The EKMS ID must be part of the short title.

b. (U) The attached media label must indicate whether or not its content(s) is/are EKMS key transactions.

c. (U) EKMS media containing encrypted key loaded from an LMD/KP will be marked with a classification of SECRET. The notice "COMSEC ACCOUNTABLE" shall also be present to indicate that the material must be tracked within the COMSEC Material Control System (CMCS). EKMS media containing unencrypted key will be classified at the level of the key (cannot be lower than SECRET due to system classification) and marked CRYPTO.

d. (U) Media containing SDNS key, STU-III key, or MSK must not be copied.

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

(2) (U) Tier 2/Tier 3 Media

(a) (U) Media containing EKMS key transactions are one-time use and must not be copied. EKMS key transactions include BETs, Individually Encrypted Transactions (IETs), and benign fill key messages. Media containing such transactions must be uploaded and destroyed within 3 working days of receipt.

(b) (U) Media containing only non-EKMS key transactions may be copied but must be accounted for individually and locally. Non-EKMS entities providing media must maintain records of all keys loaded to that media. Such media must be destroyed when no longer needed or when all key is superseded.

8. (U) Storage - Keys stored in a computer must be transferred and stored in encrypted form. The computer, other than an LMD, will be classified at the highest level of data processed/stored and protected at that level. The LMD must be classified SECRET and the data will be processed/stored and protected at that level.

9. (U) Inventory - When an inventory of electronic key is performed by an EKMS component (e.g., LMD/KP, Tier 1, etc.), a witness is not required.

10. (U) Destruction - Destruction of electronic key by an EKMS component, such as the LMD/KP or LMD-only, does not require a witness. When documenting the destruction of electronic keys at a subaccount or authorized LMD, if an electronic audit trail is not available, the COMSEC custodian/manager must maintain records certifying the destruction was performed. When documenting the destruction of electronic key issued to a DTD or non-EKMS element, the COMSEC custodian/manager must maintain hard copy records certifying the destruction (e.g., zeroization) of the key, if an electronic audit trail is not available. Media that contains SECRET or TOP SECRET data must be destroyed in accordance with NTISSI No. 4004, Routine Destruction and Emergency Protection of COMSEC Material, dated 11 March 1987.

11. (U) Reportable COMSEC Incidents - Refer to NSTISSI No. 4003, Reporting and Evaluating COMSEC Incidents, dated 2 December 1991, which contains a general listing of reportable COMSEC incidents. In addition, the following provide requirements for system-specific incidents:

a. (U) NAG-71, Interim Operational Systems Security Doctrine for the Local Management Device/Key Processor (LMD/KP) (KOK-22), dated 10 April 1997.

b. (U) NSTISSI No. 3021, Operational Security Doctrine for the AN/CYZ-10/10A Data Transfer Device (DTD), dated September 1997.

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

DISTRIBUTION:

[redacted]

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

[redacted]