



***Operational Systems Security Instruction for the
Local Management Device/Key Processor (LMD/KP) (KOK-22)***

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

This instruction implements NAG 71, *Interim Operational Systems Security Doctrine for the Local Management Device/Key Processor (LMD/KP)(KOK-22)*. It provides minimum security standards for the protection and use of the LMD/KP and associated COMSEC material. Direct questions and comments on the contents of this instruction through command COMSEC channels to Headquarters, Air Force Communications Agency (HQ AFCA), Support and Development Branch (SYSC), 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234.

1. PURPOSE AND SCOPE.

1.1. This instruction contains minimum security standards for safeguarding, controlling, and using the Local Management Device/Key Processor (LMD/KP) and associated Communications Security (COMSEC) material at Tier 2 accounts. This current version of the LMD/KP instruction is specific to Release 2.0 of the Local COMSEC Management Software (LCMS) and the associated production model KPs. As upgrades to this software/hardware are available, this instruction will be changed to reflect them.

1.2. The provisions of this instruction apply to all Air Force personnel and their contractors who handle, distribute, account for, store, or use the LMD, LCMS Release 2.0, the associated production model KP and associated COMSEC material.

2. EXCEPTIONS.

2.1. Requests for exceptions to any of the provisions of this instruction must be submitted through COMSEC channels to HQ AFCA/SYSC, 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234, for approval prior to implementation. All requests for exceptions must be accompanied by complete operational justifications.

3. SYSTEM DESCRIPTION.

3.1. Capability

3.1.1. The Local Management Device (LMD) is a user provided commercial off-the-shelf (COTS) IBM compatible personal computer running the NSA supplied Local COMSEC Management Software (LCMS). The LMD requires a STU-III or KG-84 to support Electronic Key Management System (EKMS) communications. Other cryptographic equipment (e.g. Secure Telephone Equipment (STE), KG-184 and KY-68) may be used if they are compatible with the LMD and are keyed and NSA endorsed to secure SECRET traffic. *NOTE. All references to LMD in this document denote the complete LMD platform of hardware and software.*

3.1.2. The KP, nomenclated the KOK-22/TSEC, is a cryptographic device that runs in tandem with the LMD as an integral part of the EKMS. The primary purpose of the KP is to support the LMD in implementing key management

functions such as generating key, encrypting and signing EKMS messages and issuing electronic keys to fill devices. The KP implements additional functions to ensure the security of the controlling computer/KP system (e.g., initialization, self-test, zeroization, and audit functions).

3.2. Maximum Level of Use

3.2.1. **Local Management Device** -- The LMD is operated as a SECRET high system. It is approved to process and store encrypted keying material and SECRET data. The LMD does not process or store unencrypted key.

3.2.2. **Key Processor** -- The KP is approved for use up to the TOP SECRET level including processing key of all classifications and categories. The KP interface with the LMD is Trusted to support only the transfer of SECRET data and encrypted key. All unencrypted key is distributed through the KP's six pin fill device interface.

4. KEYING.

4.1. **Controlling Authority** -- AFI 33-215, *Controlling Authorities for COMSEC Keying Material*, describes responsibilities of organizations that serve as controlling authorities for COMSEC keying material, and provides guidance for fulfilling those responsibilities.

4.2. **Key Types** -- There are four categories of keys handled by the KP: (1) keys used for EKMS messages (EKMS Message Signature keys), (2) keys needed for the KP's own internal use (KP Internal keys), (3) keys used for COMSEC equipment internal to EKMS (e.g. STU-III), and (4) keys handled (i.e., generated, encrypted, decrypted, stored and issued, as appropriate) by the KP for use in cryptographic devices, equipment, or systems (user keys) outside EKMS.

4.2.1. EKMS Message Keys

4.2.1.1. **KP FIREFLY Key** -- EKMS FIREFLY key is used for LMD/KP to LMD/KP or LMD/ KP to Central Facility (CF) key distribution. The EKMS FIREFLY key is generated by the CF and filled into a KP, whether from a KSD-64A (for seed key) or electronically (for operational key). This KSD-64A also contains the EKMS ID of the element where it is to be used and the classification level of the FIREFLY key.

4.2.1.2. **Message Signature Key (MSK)** -- MSK is used to cryptographically "sign" EKMS messages. This "signature" provides authentication of messages. The EKMS MSK is generated by the Central Facility and filled from a KSD-64A. EKMS MSKs are to be protected at the SECRET level.

4.2.1.3. **Destruction of KP FIREFLY and MSK** -- Once these keys are inserted into the LMD/KP, a backup should be performed. KSD-64As containing EKMS MSKs, FIREFLY keys and Privilege Certificates used in the KP, must then be zeroized three times in a STU-III. They are not to be kept locally in unencrypted form, but are kept encrypted on the LMD, allowing recovery from the backup if the LMD fails.

4.2.1.4. **EKMS STU-III Key** -- When a STU-III is used for EKMS purposes, the STU-III must be keyed with key specifically ordered for EKMS usage. The key must be classified at least at the SECRET level.

4.2.2. **KP Internal Keys** -- There are several keys that the KP generates and uses internally which the user never encounters directly, but are affected by certain LMD/KP functions/processes. These functions/processes are: Site Reinitialization, Changeover, and KP Rekey.

4.2.2.1. **Site Reinitialization** -- The Site Reinitialization process enables the recovery of all protected data stored on the LMD and is used when a KP must be replaced with a new KP due to failure or recertification.

4.2.2.2. **Changeover** -- Changeover is the process used in order to reencrypt the LMD database when the cryptoperiod of the Local Key Encryption Key (LKEK) expires. The LKEK has a cryptoperiod of three months. The process of reencryption and supersession is an automatic background operation of the LMD/KP but must be initiated manually.

4.2.2.3. **KP Rekey** -- The Reinit1 and Reinit2 KSD-64As are created during Site Initialization and used in the site reinitialization and changeover processes. The Reinit1 and Reinit2 KSD-64As must be protected to the highest classification level of the EKMS element.

4.2.3. **Benign Fill (BF) Keys** -- The BF keys are used to encrypt the link between the KP and a BF capable end equipment for the purpose of keying the end equipment. These keys are created by the CF, will be labeled with the appropriate classification and must be protected to that level.

4.2.4. **User Keys** -- Instruction for user keys is addressed in instruction for individual equipment.

4.3. **Credentials** -- Credentials will need to be posted to the CF or other EKMS elements, depending on user key requirements. Each credential may be used for a maximum of one month. Users may make an initial posting of two credentials. Credentials, which are created by a FIREFLY key, expire automatically when the associated FIREFLY key expires. Use of up-to-date credentials is mandatory at all levels. It may be useful for some users (e.g. those being deployed) to rekey before the end of their FIREFLY key's cryptoperiod and post a new set of credentials.

NOTE: Credentials are not key and, therefore, do not have a cryptoperiod. Credentials do, however, have expiration dates.

4.4. **Cryptoperiods and Source Information** -- See Section D.

5. RESTRICTIONS.

5.1. **Personnel** -- LMD/KP systems must only be operated by authorized individuals who have been assigned key management responsibilities. These individuals must have a minimum of a SECRET clearance and be enrolled in the Cryptographic Access Program (CAP). TOP SECRET clearances are necessary to output unencrypted TOP SECRET key as well as to input or output encrypted key at a TOP SECRET account. Persons assigned primary responsibility for the key processed by the LMD/KP must be adequately trained in both LMD/KP operations and in proper security procedures. Procedures must be in place to promptly terminate system access once an authorized user is relieved of his/her responsibilities.

5.2. **Local Management Device** -- The LMD must be operated consistent with AFSSI 5102, *The Computer Security (COMPUSEC) Program*, and local procedures for Automated Information Systems (AIS) which are SECRET system high. LMD's are designed to process SECRET data on a standard stand-alone computer platform with or without a KP, and to support dial-up communications with other EKMS elements. The LMD is not designed to handle unencrypted keying material. Any change to the configuration requires recertification and accreditation by the cognizant Designated Approving Authority (DAA). The following minimum restrictions apply to both LMD/KP and LMD only accounts:

5.2.1. **Non-LCMS Software** -- Non-LCMS software (e.g. word processing software) to be used on the LMD must be approved by the appropriate security officer and DAA who must make a risk management decision based on the threat to and the vulnerability of the LMD. DAAs may contact their Wing or MAJCOM IP Office for guidance.

5.2.2. **Software Compilers** -- Software compilers are prohibited on the LMD.

5.2.3. Only NSA approved software may be electronically transmitted between EKMS components. Signed DTD software has been NSA approved.

5.2.4. Neither the LMD nor the KP may be connected to any Local Area Network (LAN).

5.2.5. **LMD Communications** -- NSA-approved Type I encryption devices or protected distribution systems must be used to provide security for all LMD transmissions over a communications circuit. Such Type I encryption devices must be compatible with the LMD, as well as keyed and NSA endorsed to secure SECRET traffic. EKMS network traffic must be encrypted during transmission in accordance with the SECRET system high classification level. STU-III equipment are the cryptographic equipment of choice whenever possible because the display provides an additional level of authentication. Where such authentication is not possible (e.g., KG-84A/84C), the user and DAA must assume the additional risk or take other measures to ensure all traffic is authenticated. *NOTE: Cryptographic Units other than the STU-III and KG-84A/84C might not be compatible with the CF.*

5.2.6. **LCMS Audit data**

5.2.6.1. LCMS audit records must be periodically reviewed for anomalies. These anomalies could include instances of multiple invalid logon attempts, invalid file access attempts, operators logging on at unusual times, excessive

transfer of keys to DTDs or other fill devices, etc. The use of NSA's Audit Reduction Analyzer tool is highly recommended, for use by audit teams. It is suggested that the LCMS audit data be reviewed at least monthly, and that audit teams review the data at least yearly.

5.2.6.2. LCMS audit data and accounting records must be held until the next Central Office of Record (COR) audit. They may be kept off-line on a separate disk, tape, etc. See also paragraph 7.3.3.3 on archive.

5.2.6.3. Individuals who analyze LCMS audit data must be knowledgeable in LMD/KP operations and trained to detect and respond to anomalous events. Access to audit data must be restricted to authorized individuals.

5.2.6.4. Operators should not normally be allowed read access to their own security event audit data. For small accounts, e.g., some Air National Guard accounts, with no knowledgeable individuals other than the COMSEC manager and alternates, the COMSEC manager may review the audit data monthly with periodic (yearly suggested) audits to be performed by an independent, outside auditor representing Command Headquarters.

5.2.6.5. LMD/KP audit data is considered SECRET.

5.2.6.6. **Viruses And Other Malicious Code** -- Viruses and other malicious code are a threat to the confidentiality, integrity and availability of the EKMS system. The following is informal guidance only and currently has minimal application to UNIX platforms. UNIX platforms with a DOS partition are susceptible to the many DOS viruses.

5.2.6.6.1. In keeping with good computer security practices, all software should be initially checked for viruses and other malicious code prior to loading onto the EKMS system. All data disks should be checked for malicious code prior to loading and the EKMS system should be checked periodically for viruses and other malicious code. The strictness of this check and the schedule on which it is performed depend upon the trust of the operating system (e.g. UNIX vs. DOS), the threat to the operating system and database, and the availability of appropriate tools. Prudence must be used by the operators of the LMD/KP to ensure the absence of viruses and other malicious code within the system and all software/files brought in from outside the system.

5.2.6.7. **LMD Power-up**

5.2.6.7.1. The LMD must boot from its removable hard drive as its default. Booting from devices such as a floppy disk, CD-ROM and tape are permissible for installation, upgrade and system maintenance only.

5.2.6.7.2. Perform monthly file integrity checks. This performs a check of the LCMS software to ensure that it has not been inadvertently corrupted or maliciously changed. *NOTE. This check is of the LCMS software only. It does not check the LCMS database.* If the check has a negative result, notify the System Administrator, investigate the cause of the problem, and reload the LCMS software.

5.3. **Copying Key** -- The EKMS is designed to send only one copy of a key to each location where copies are made as needed. Care must be taken to comply with current procedures in assigning key to cryptonets and specific equipment.

5.3.1. Each cryptonet or point-to-point circuit must be secured with a key distinct from that used on any other cryptonet or point-to-point circuit unless specific equipment systems instruction allows otherwise.

5.3.2. Copies of operational FIREFLY (asymmetric or "modern") key may not be used. When transferring (copying) operational FIREFLY key from a DTD to COMSEC equipment (e.g., a KG-75), the copy remaining in the LMD or DTD must be not be used to key another equipment. It may be retained for rekeying the same equipment in case of inadvertent zeroization. See AFSSI 3021, *Operational Security Doctrine for the AN/CYZ-10/10A Data Transfer Device*, for length of time key may remain in the DTD. Test FIREFLY key may be copied and accounted for locally within one COMSEC account. If transferred from that account, all copies must be destroyed.

6. **CLASSIFICATION/MARKING/ACCOUNTABILITY.**

6.1. AFMAN 33-272 (S), *Classifying Information Protection Information (U)*, provides general classification guidance for COMSEC information. Guidance for specific equipment can be found in the instruction for that equipment. The following additional guidance also applies:

6.2. **KP**

6.2.1. The baseline classification of a KP is SECRET, ALC 1 (accountable by serial number) when unkeyed (CIK not inserted) or zeroized, and when only one operator is logged-on.

6.2.2. When keyed with two CIKs whose users are cleared and designated TOP SECRET, the KP becomes TOP SECRET CRYPTO since it can process and output TOP SECRET CRYPTO key in unencrypted form. *NOTE: The LMD remains SECRET in this mode since the KP is trusted not to output TOP SECRET key/data to the LMD.*

6.2.3. **CIKs** -- All KP CIKs, including Transit CIKs, System Administrator CIKS, and user CIKs, are classified SECRET. They may be declassified when they are disassociated (i.e., deleted) from the KP. The Transit CIK is generated at the manufacturer or depot as an ALC 4 item, initial receipt required. System Administrator CIKS, and user CIKs are generated locally and are not assigned an ALC, but still require local accounting.

6.2.4. **KP Personal Identification Numbers (PIN)** -- PINs are classified SECRET for SECRET operators, TOP SECRET for TOP SECRET operators.

6.2.5. Limit access to each CIK and its associated PIN. The KP assigns each CIK a unique PIN.

6.3. Key

6.3.1. See Section D for a summary of marking and accountability information for KP key.

6.3.2. **KP-Generated** -- KP-generated key may be classified up to TOP SECRET, will be "marked" CRYPTO and assigned ALC 6 (continuous accountability to the COR) or ALC 7 (continuous local accountability within the EKMS).

6.3.3. **User Keys** -- User keys that are output in unencrypted form are classified at the highest level of information they protect. User keys that are output in encrypted form are UNCLASSIFIED CRYPTO. Keys should be output from the KP in encrypted form unless operational requirements dictate otherwise.

6.3.4. **STU-III/KG-84 Key** -- Key for the STU-III or KG-84 (or other authorized equipment) used to transfer key and other EKMS data between EKMS elements must be classified a minimum of SECRET CRYPTO. The STU-III, if used, may also be employed for non-EKMS use (see paragraph 7.4.1.2).

6.3.5. **Magnetic Media** -- Any magnetic media used to transport encrypted key is classified SECRET and handled as an ALC 4 item. EKMS encrypted key on magnetic media (e.g., floppy disks), sent to an EKMS account with an LMD/KP, must be reconciled within three working days of receipt. This allows time for the key to be decrypted by the KP, verified correct and reencrypted in the LKEK. This must be done since the LMD/KP can not verify the contents of the floppy disk unless it decrypts the key.

6.3.6. **Handling** -- COMSEC Managers supporting LMD/KP systems must handle and account for electronic keys as virtual rather than physical items. This means that the COMSEC Manager must assume that all key listed on the Central Facility/COR/LMD generated Transfer Initiating, Transfer Receipt, and Destruction Reports have been received, transferred, issued, or destroyed if the LMD/KP identifies them as such.

6.4. **LCMS** -- The LCMS is classified SECRET.

6.5. LMD

6.5.1. Once the LCMS is loaded onto the LMD platform, the LMD becomes SECRET. The LMD is not designated CRYPTO. (RATIONALE: The KP is trusted to never allow unencrypted key to be copied to the LMD. Also, while encrypted keys (which are UNCLASSIFIED CRYPTO) reside on the LMD hard drive, the LMD classification is already SECRET, requiring more restrictive handling than for UNCLASSIFIED CRYPTO.)

6.5.1.1. TOP SECRET data and unencrypted key are not allowed on the LMD. If inadvertently placed on the LMD, all prudent measures must be taken to remove it. Such measures must be determined by the local cognizant security authority. Until removal can be verified, the LMD should be treated at the level of the unencrypted key (up to TOP SECRET). *NOTE. Encrypted TOP SECRET key sent from the KP to the LMD is UNCLASSIFIED CRYPTO. (Care should be taken to ensure that no connection exists between the LMD and a TOP SECRET system/device other than the KP. Floppy disks introduced to the LMD should likewise be no higher than SECRET.)*

6.5.2. LMD passwords are classified SECRET.

6.5.3. All media (electronic, magnetic, etc.) that comes from or in contact with an LMD must be classified SECRET and handled as ALC 4 items. Paper printouts may be physically reviewed and downgraded as appropriate.

Magnetic media (e.g., diskettes) may be declassified, if authorized by the local security authority, by following locally allowable procedures and using local tools for declassifying such media. *NOTE: This does not apply to the DTD. See AFSSI 3021.*

6.5.4. Peripheral equipment with internal storage must be classified SECRET, with the exception of the DTD.

6.5.5. Privilege Certificates are For Official Use Only (FOUO), ALC 4 if loaded onto a KSD-64A. Privilege Certificates can also be sent electronically through EKMS.

6.5.6. All fill devices and the AN/CYZ-l0 Data Transfer Device (DTD) are Controlled Cryptographic Items (CCI). Refer to AFSSI 3021 for guidance on the DTD's classification.

7. PHYSICAL SECURITY.

7.1. AFKAG-1 describes the minimum standards for safeguarding and controlling classified COMSEC equipment and keying material, and also prescribes the standards for safeguarding COMSEC facilities operated by the U.S. Government or by contractors in connection with U.S. Government contracts. AFI 33-203, *The Air Force Emission Security Program*; AFSSI 7010 (S), *The Emission Security Assessment (U)*; and AFSSM 7011, *The Emission Security Countermeasures Review*, establish guidelines, restrictions, and procedures for determining the applicable countermeasures for equipment, systems, and facilities that process national security information. AFI 21-109, *Communications Security (COMSEC) Equipment Maintenance and Maintenance Training*, establishes minimum standards, delineates responsibilities, and establishes procedures for COMSEC equipment maintenance and maintenance training. In addition, the following specific physical security requirements also apply:

7.1.1. The System

7.1.1.1. The LMD/KP system, including connecting cables, must be located in an area where it will receive at least SECRET level protection during operation. (See paragraph 7.7 for storage requirements.) Area controls must be sufficient to prevent unauthorized access to the system and to keying material processed by it (see AFSSI 7010 and AFSSM 7011 for details). Consult AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III), Type I* for guidance on connecting and using the STU-III with the system.

7.1.1.2. Since authentication information, warnings and instructions appear on the KP display, the STU-III display and the LMD computer screen, these system components must be arranged so that the displays are clearly visible to the system operator.

7.1.1.3. System Administrators and operators must be cleared to the highest level of key that they can access, with a minimum of SECRET. In addition, those whose official duties require continuing access to unencrypted SECRET CRYPTO or TOP SECRET CRYPTO keying material are subject to the requirements of AFKAG-1.

7.2. **Operator Privilege Management** -- Operator privileges are assigned at the system level and should be commensurate with that operator's job responsibilities. Although multiple System Administrators may be appointed for an organization, appointments should be limited to only those administrators needed by the site (e.g., one per shift).

7.3. Equipment

7.3.1. Key Processor

7.3.1.1. **Recertification** -- KPs must be recertified on a regular basis or whenever they are repaired, but not later than once every three years. Keep shipping documents to verify the date of last recertification. If the KP low battery light illuminates, plans should be immediately made to send the unit to the depot for replacement and recertification. The KP may be used while plugged into AC power, which prevents automatic zeroization due to low power.

7.3.1.2. **Personal Identification Number (PIN)** -- PINs for the KP must be safeguarded in accordance with their classification. Access to a stored PIN must be restricted to the individual to whom it is assigned. PINs must be changed every six months.

7.3.1.3. **Keyed KP** -- A keyed KP (CIK inserted) must be protected in accordance with its classification.

7.3.1.4. **Evidence of Tamper** -- If there is evidence of tamper of the KP (e.g., unexplained zeroization, damaged seals, drilled out screws), the KP must not be used. Evidence of tampering is a reportable COMSEC incident (see paragraph 9 below).

7.3.1.5. **Failed KP** -- When a KP failure occurs, it must be replaced with a KP that has not already been Site Initialized. An LMD/KP System Administrator will perform the KP Reinitialization process. This process requires Reinit1, Reinit2 (See paragraph 4.2.2.1 and 4.2.2.3 above), and the current LCMS.

7.3.1.6. **Two Person Integrity (TPI)** -- Two appropriately cleared KP operators must be physically present when the KP is keyed to output unencrypted TOP SECRET key (two CIKs have been inserted) or when outputting key designated as TPI. An operator who is authorized (privileged) TOP SECRET may use the KP in the SECRET mode without TPI, but once the operator desires to output unencrypted TOP SECRET key, the TPI mode must be entered and the KP must be considered TOP SECRET, with two operators present. The KP reverts to SECRET upon exiting from the TPI mode, graceful shutdown of the KP or zeroization of the KP. TPI also does not apply to processing of TOP SECRET benign key, which can be done with only one operator since benign key is never in unencrypted form.

7.3.2. **KP CIKs**

7.3.2.1. All KP user CIKs are SECRET and must be protected accordingly. All user CIKs must be protected to ensure individual accountability, that is, the individual is responsible for knowing its whereabouts. The number of user CIKS assigned to each KP should be kept to a minimum.

7.3.2.2. KP CIKs are loaded on KSD-64A devices. These are the same devices used in the STU-III and other equipment. When the KP CIKs are zeroized (e.g., three times in a STU-III), they are unclassified and may be used in other COMSEC equipment. Conversely, KSD-64As which have previously been used in other COMSEC equipment may be used as KP CIKs after appropriate zeroization. Excess KSD-64A devices should be returned to the CF for reuse. They must be properly zeroized prior to any shipment.

7.3.3. **Local Management Device**

7.3.3.1. The LMD must be protected in accordance with its classification.

7.3.3.2. **Backup**

7.3.3.2.1. Data backups are necessary to recover from local failures of the system. The more data on the system, the greater the need for, and the more frequent should be, the backups. Perform backups as follows: new LCMS data daily, full LCMS data backup weekly, and a full system backup when the system is first installed and then monthly thereafter.

7.3.3.2.2. The files (including the database of encrypted key files) on the LMD may be backed up individually or in a more automated fashion. At the very least, the existence of backups should be documented in a facility security plan approved by the facility security officer or COMSEC Manager, giving labeling information, storage location, classification, responsible personnel, etc. Local accountability per item should be maintained until the next command COMSEC audit/functional review, showing identification of the source material (short-title and, if possible, edition), number of copies made, to whom the material was issued, and disposition.

7.3.3.2.3. If it becomes necessary to restore the LCMS database from a backup file, keys received since the last backup will be lost, and keys previously destroyed will reappear. This is not a COMSEC incident, but if repeated, should be investigated. The operator and System Administrator should make a good faith effort to immediately destroy all superseded key, and request new copies of recently received key.

7.3.3.3. **Archive** -- Accounting and audit data should be archived when no longer needed (i.e., after command COMSEC audit/functional review). Archive data will be kept 30 years for compromise purposes.

7.4. **Communications Devices**

7.4.1. **STU-III**

7.4.1.1. When keyed with EKMS identified key (EKMS CIK inserted), the STU-III may only be used by persons who are authorized to use the EKMS system. The EKMS key is required for authentication purposes during LMD/KP to LMD/KP (or LMD to LMD/KP) communications as well as LMD/KP to CF communications.

7.4.1.2. The STU-III may be used for non-EKMS use. This can be done using the EKMS key (at the SECRET or higher level), or using another key in the same STU-III. The non-EKMS key must be accessed by use of a separate

CIK. This non-EKMS CIK may be used by non-EKMS users. When the STU-III is used for non-EKMS purposes, the LMD must be disconnected or turned off.

7.4.1.3. The use of SACS is optional for attended STU-III use with an LMD/KP. Unattended STU-III use with an LMD/KP is prohibited. Use of STU-III Access Control System (SACS) features is highly recommended. The SACS Minimum Security Level should be set at SECRET. The SACS Maximum Security Level need not be set, allowing two users with TOP SECRET key to go secure at that level. Going secure at the TOP SECRET level will not change the classification of the SECRET LMD since only SECRET high information will be accessed/passed.

NOTE: Depending on the vendor of the STU-III, there may be up to four keys in a STU-III. The SACS features may be set once for the telephone and enabled separately for each key, or they may be set separately for each key depending upon make/model of the telephone. See each vendor's operator handbook.

7.4.1.4. The SACS Access Control List may be used to limit the set of equipment with which an equipment will go secure. If the List is not used, visual sighting of the STU-III EKMS ID is required for each use of the STU-III to ensure connection to a valid EKMS account.

7.4.2. **KG-84A/84C** -- Consult AFSSI 3017, *Operational Security Doctrine for Stand Alone KG-84, KG-84A, and KG-84C*, for guidance on physical security of these equipment. In order for a KG-84A/84C to be employed for non-EKMS use, it would need to be disconnected from the LMD/KP and rekeyed. KG-84A/84C equipment are anticipated to be dedicated for EKMS use.

7.4.3. **Fill Devices** -- Consult AFSSI 3021 for guidance on physical control of the DTD. Keyed KYK-13s and KYX-15s must be protected commensurate with the classification of the stored key.

7.5. Transportation

7.5.1. All key production equipment including KPs must be transported by Defense Courier Service (DCS) or cleared courier. Consult AFKAG-1 for additional instructions. Transport of other EKMS equipment must be according to AFKAG-1.

7.5.2. The KP must be packaged and shipped separately from any of its associated CIKs. It must also be shipped separately from its KSD-64A's containing Reinit1 and Reinit2. The KP must be zeroized prior to shipment for maintenance or recertification unless the equipment is malfunctioning and unable to be zeroized.

7.5.3. In the event that a KP becomes inoperable and the operator is unable to confirm that the KP has been zeroized, then the KP CIK should be zeroized (e.g. three times in a STU-III) and the equipment sent via DCS back to the depot.

7.5.4. KPs and LMDs used in transportable/mobile COMSEC facilities need not be removed or zeroized prior to relocation of the facility to another site; however, the KP must be unkeyed (CIK removed). During movement of the facility (with an LMD/KP inside) to another site, the facility must be secured with a GSA-approved lock and escorted. Alternatively, the LMD/KP may be secured in GSA-approved security containers. Escorts need not be armed, but must be cleared for classification of COMSEC material contained in the facility.

7.5.5. Software used on the LMD must be distributed via approved methods.

7.6. Maintenance

7.6.1. The KP will be maintained at HQ Cryptologic Systems Group (CPSG) only.

7.6.2. Maintainers of the LMD computer software, and storage media must have at least a SECRET clearance. Since the LMD computer is not a COMSEC item, COMSEC maintenance requirements do not apply.

7.7. **Storage** -- The LMD and KP must be stored either in an area approved for open storage of at least SECRET material, or the LMD's hard drive may be removed and properly stored (e.g., in a GSA approved safe) along with the KP. Access to the area or safe must be limited to at least SECRET cleared individuals.

7.8. **TEMPEST Considerations** -- Using organizations must consult AFSSI 7010 (S), *The Emission Security Assessment (U)*, and AFI 33-203, *The Air Force Emission Security Program*, to determine applicable countermeasures for the LMD and for the facility in which it is placed.

8. ROUTINE DESTRUCTION AND EMERGENCY PROTECTION.

8.1. AFKAG-1 and AFI 33-211 prescribe standards for disposition of COMSEC material, and provide criteria and guidance for protecting COMSEC material under emergency conditions. It also provides guidance and assigns responsibilities for recovery of abandoned COMSEC material. The following specific standards also apply:

8.2. Electronic Key

8.2.1. The LMD/KP audit keeps track of destroyed electronic key. This is sufficient for electronic key destruction in LMDs at elements that have a KP.

8.2.2. Witnessing is not required for destruction or inventory of electronic key where the destruction or inventory is performed by the LMD/KP. However, witnessing continues to be a requirement for any COMSEC material used in EKMS that must be physically destroyed and/or inventoried.

8.2.3. The LMD/KP will not allow reuse of a key package on a floppy disk, so the encrypted key on the floppy disk must be "destroyed" after uploading the keys to the LMD/KP. In order to destroy the keys, the media may be destroyed, degaussed or overwritten in accordance with AFSSI 5020, *Remanence Security*. Media produced by the Central Facility or the LMD may be either destroyed, or, if desired, degaussed or overwritten for reuse in the transmission of EKMS key or key related data, and classified SECRET. Any other use is prohibited. It is not necessary to verify sanitization if the floppy is to be shredded in accordance with regulations for shredding a floppy disk which contains classified SECRET data (disregarding any unclassified CRYPTO marking).

8.3. Emergency Destruction

8.3.1. In case of imminent hostile takeover, the KP should be zeroized before attempting to destroy the LMD because the KP is more critical to EKMS security. Unencrypted key should be destroyed before encrypted key.

8.3.2. In order to zeroize the KP, rapidly depress the zeroize switch three times (within 6 seconds). The 'ZEROIZED' LED lamp must light. *Note: If on battery power, the lamp will only light for one second.* If the LED does not light, consider the KP broken, not zeroized.

9. REPORTABLE COMSEC INCIDENTS.

9.1. AFI 33-212, *Reporting COMSEC Incidents*, contains a general listing of reportable COMSEC incidents and the standards for reporting them. Additional reportable COMSEC incidents, specific to the KP follow:

9.1.1. Loss, or compromise, of any of the following;

9.1.1.1. KP CIKs and non-zeroized KP KSD-64As (e.g., Reinit1 and Reinit2).

9.1.1.2. KP keys (EKMS FIREFLY and EKMS MSK).

9.1.1.3. Floppy disks containing key or other EKMS information.

9.1.1.4. Detection of malicious code on the EKMS system.

9.1.1.5. KP PINS.

9.2. **Unaccountable KP Zeroization** -- If the KP is found to be zeroized and the event is unaccountable (i.e., no one claims responsibility), a COMSEC incident report must be made to cover the possibility of tamper before the KP is returned to depot for reinitialization.

9.3. **Inexplicable KP Damage** -- If the KP is found to be physically damaged, a COMSEC incident report must be made to cover the possibility of tamper, and the KP must be returned to depot.

GEORGE L. FIEDLER, Lt Col, USAF
Chief, Networks Division

For Official Use Only

Directorate of Systems, AFCIC

4 Encls:

1. Section A -- References
2. Section B -- Acronyms and Abbreviations
3. Section C -- Terms
4. Section D -- Classification and Handling of Key and Privilege Certificates

GLOSSARY OF REFERENCES, ACRONYMS, ABBREVIATIONS, AND TERMS

Section A -- References

AFI 21-109, *Communications Security (COMSEC) Equipment Maintenance and Maintenance Training*
 AFI 31-501, *Personnel Security Management Program*
 AFI 33-203, *The Air Force Emission Security Program*
 AFI 33-209, *Operational Instruction for the Secure Telephone Unit (STU-III) Type I*
 AFI 33-211, *Communications Security (COMSEC) User Requirements*
 AFI 33-212, *Reporting COMSEC Incidents*
 AFI 33-215, *Controlling Authorities for COMSEC Keying Material*
 AFKAG-1, *Air Force Communications Security (COMSEC) Operations*
 AFKAG-2, *AF COMSEC Accounting Manual*
 AFMAN 33-270, *Command, Control, Communications and Computer (C4) Systems Security Glossary*
 AFMAN 33-272 (S), *Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information (U)*
 AFSAL-4001, *Controlled Cryptographic Items (CCIs)*
 AFSSI 3017, *Operational Security Doctrine for Stand Alone KG-84, KG-84A, and KG-84C*
 See AFSSI 3021, *Operational Security Instruction for the AN/CYZ-10/10A Data Transfer Device*
 AFSSI 3030, *Protected Distribution System*
 AFSSI 5020, *Remanence Security*
 AFSSI 7010 (S), *The Emission Security Assessment (U)*
 AFSSM 7011, *The Emission Security Countermeasures Review*

Section B -- Acronyms and Abbreviations

AFI	Air Force Instruction
AFMAN	Air Force Manual
AFSSI	Air Force Systems Security Instruction
AFSSM	Air Force Systems Security Memorandum
AIS	Automated Information System
ALC	Accounting Legend Code
BF	Benign Fill
CAA	Controlled Access Area
CCI	Controlled Cryptographic Items
CF	Central Facility
COR	Central Office of Record
DAA	Designated Approving Authority
DCS	Defense Courier Service
DTD	Data Transfer Device
EKMS	Electronic Key Management System
EMSEC	Emission Security
IP	Information Protection
LKEK	Local Key Encryption Key
LMD/KP	Local Management Device/Key Processor
LCMS	Local COMSEC Management Software
MAJCOM	Major Command
MSK	Message Signature Key
OSHA	Occupational Safety and Health Act
PDS	Protected Distribution System
STE	Secure Telephone Equipment
STU	Secure Telephone Unit
TEMPEST	Control of Compromising Emanations from Message Processing Hardware

Section C -- Terms

ALC-6 - Electronically generated key that is continuously accountable to a Central Office of Record (COR) by means of the Electronic Key Management System (EKMS). Similar to electronic ALC-1.

ALC-7 - Electronically generated key that requires continuous local accountability. Similar to electronic ALC-4.

Associated Key - All keys loaded into a DTD by each CIK are associated with that CIK.

Black - Designation applied to telecommunications and automated information systems, and to associated areas, circuits, components, equipment, and wirelines in which only unclassified signals are processed.

COMSEC Side - The COMSEC side performs the cryptographic functions used to decrypt key, store key, create and store audit data, and control uploads and downloads.

Continuous Protective Custody - DTDs and CIKs must be in the control of authorized personnel at all times. This includes during use and during storage.

Credential - The FIREFLY exchange information required by another element in order for both elements to cooperatively generate the same session key.

Crypto-Ignition Key (CIK) - The DTD CIK is used in the DTD to access key and initiate security functions.

Downloading - Transferring software or Host side data to the DTD.

EKMS Element - EKMS functional entity at a single site which has been assigned an EKMS ID and which is supported by one or more EKMS components that perform specified key management functions.

Group CIK - These are multiple CIKs that use the same LKEK as established by the Local Management Device/Key Processor (LMD/KP).

Host Side - The Host Side is used to store and execute application software, store unencrypted data (e.g., Signal Operating Instructions), and Benign Fill messages.

INFOSEC Software - computer or microprocessor instructions and/or routines used in the LMD which control or perform INFOSEC and INFOSEC related functions, e.g., the Local COMSEC Management Software (LCMS).

Initialized CIK - A CIK that has gone through the randomization process and is now associated with a particular DTD allowing access to that DTD. It has a specific Local Key Encryption Key (LKEK) associated with that CIK, and will only allow access to key loaded by that CIK.

Key Deletion - This deletes an individual key from the DTD.

Key Fill - When an electronic key is loaded to make it operational in the DTD or an end equipment.

Key Issue - When electronic key is transferred between EKMS components for transport or storage.

Key Storage Device (KSD) - A specific physical device which can be used as a fill device and also as a crypto-ignition key (CIK) in the KP. Presently the KSD in the EKMS system is used as a fill device to transfer key from the Central Facility to the depot and/or user. Future enhancements to EKMS may allow the KP to load key into a KSD for subsequent load into an end cryptographic unit.

Keyed - A Keyed DTD has the associated, initialized CIK inserted.

Keyed KP - A KP that contains key and in which a valid CIK has been inserted. A KP which has been depot initialized, but not yet site initialized, is considered keyed if the transit CIK is inserted.

KP Privilege Certificate - An access control mechanism, consisting of a list of element-specific data and privileges provided by the account's Privilege Certificate Manager on a KSD-64A, floppy disk, or electronically. This data/privileges must be installed at KP site initialization for the establishment and enforcement of the KP's ID, Highest Classification Indicator (HCI), and privileges.

Supervisory CIK - This is a CIK that has extra privileges given to allow special functions (e.g., uploading and checking audit data).

Unkeyed KP - A KP that does not contain key or from which the CIK has been removed.

Unkeyed - An Unkeyed DTD does not have its associated CIK inserted in it.

Uploading - Moving Host side data or Audit data from the DTD to a computer.

Zeroization - Zeroizing the DTD deletes all Host data, zeroizes or destroys all key contained in the DTD, and deletes all CIK associations.

Section D Classification and Handling of Key and Privilege Certificates.

Type	Classification	CRYPTO	Account ability	Cryptoperiod	Cryptonet Size	Source	Comments
Operational EKMS FIREFLY Key	SECRET or TOP SECRET	Yes	ALC 1	1 Year	Unique	Central Facility	(Notes 1 and 2)
Operational EKMS Message Signature Key (MSK)	SECRET	Yes	ALC 1	Indefinite	Unique	Central Facility	(Note 1)
Privilege Certificates	FOUO	No	ALC 4	Indefinite	N/A	Central Facility or Authorized Ordering Privilege Manager	If in physical form on a KSD-64A. (Note 1)
REINIT1 KSD-64A	SECRET or TOP SECRET	Yes	ALC 1	Automatically changed when KP is reinitialized	Unique	Local KP	Used to rebuild LKEK in a replacement KP. (Note 2)
REINIT2 KSD-64A	SECRET or TOP SECRET	Yes	ALC 1	Automatically changed at KP reinitialization and LKEK changeover	Unique	Local KP	Used to rebuild LKEK in a replacement KP. (Note 2)
Transit CIK	SECRET	No	ALC 4	N/A	Unique	Local KP	Converted to first KP CIK during initialization/ re-initialization. (Note 3)
KP User and System Administrator CIKs	SECRET	No	Local	Indefinite	Unique	Local KP	

Notes:

1. KSD-64A containing this key/data must be zeroized as soon as site initialization is complete.
2. Classified according to the highest level of key the KP is allowed to output unencrypted, minimum of SECRET.
3. The Transit CIK is normally effective only for the time it takes to ship a KP from the manufacturer or depot to a user where it will be site initialized. If the KP is put in storage, the Transit CIK may be valid for up to three years, when the KP must be recertified.