

RECORD OF AMENDMENTS

[illegible]



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
5500
ARS
14 APR 2014

From: Director, Administration and Resource Management Division
To: Distribution List

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND
DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

Ref: (a) EKMS 1 (series)
(b) OPNAVINST 2221.5 (series)
(c) SECNAVINST 5510.30
(d) Security Note 06-11
(e) EKMS 5 (series)
(f) EKMS for CO's Handbook
(g) USMC ECSD 005 (series)

Encl: (1) Nomination as Staff Agency/Activity Security Coordinator and
Local Element Control Officer
(2) Primary/Alternate Local Element Control Officer Letter of
Appointment
(3) SD Form 572 Cryptographic Access Certification and Termination AMD 1
(4) Request for Authorization to Draw COMSEC Material Form
(5) Modern Key Tracker
(6) Agreement to Hand-carry Classified Material
(7) Security Services Form
(8) Request for Residential Secure Telephone Equipment (STE)
(9) Emergency Action Plan for Communications Material System
(10) Request for Communications Security (COMSEC) support letter
(11) Required derivative statement for SF-700 Envelope [AMD 1] AMD 1

1. Purpose. To establish policies and procedures as outlined in the references, for the handling, accountability, distribution, and destruction of communications security (COMSEC) material to all Headquarters Marine Corps COMSEC users. These Standing Operating Procedures (SOP) pertains to accounts established as local elements (LEs) responsible to the Electronic Key Management Systems (EKMS) Primary Account or parent EKMS account, 169078, Headquarters, United States Marine Corps.

2. Cancellation. SOP for the Handling, Accountability and Disposition of Communications Security Material dated 24 May 2012.

3. Background. In accordance with reference (a), COMSEC material is the material used to protect U.S. Government transmissions, communications, and the processing of classified or sensitive unclassified information related to national security from unauthorized persons and the material used to ensure the authenticity of such communications. EKMS is an interoperable collection of systems, facilities, and components developed by services and agencies of the U.S. Government to automate the planning, ordering, filling, generation, distribution, accountability, storage, usage, destruction, and management of electronic key and other types of COMSEC material. The operating principles of Communications Material System (CMS) and EKMS are interchangeable, the same safeguards and applied security methodology applies equally to both which are as follows:

a. A continuous chain of custody receipts by use of transfer reports and local custody documents.

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

b. Positive accounting records, such as periodic inventory reports, destruction records, transfer reports, and local custody records.

c. The requirements for the immediate reporting of COMSEC material insecurities, COMSEC incidents, and Practices Dangerous to Security (PDS).

4. Action. All HQMC personnel, military, civilian, government contractors, and any other individual authorized access to COMSEC equipment or keying material (Keymat) distributed through the primary HQMC EKMS account will comply with the provisions of this document. This SOP cannot address every conceivable situation that might arise in day-to-day operations. The basic principles of security and proper accounting, coupled with sound judgment and common sense should always be exercised when dealing with COMSEC material. You can also contact a HQMC EKMS Manager for further assistance, at (703)614-2305, or via email at SMB_HQMC_COMSEC@USMC.MIL.

5. Responsibilities

a. Commanding Officer (CO). The Director, Headquarters Marine Corps Staff (DMCS) is the CO of this account. As such, DMCS is directly responsible for properly administering this EKMS account and ensuring compliance with established policies and procedures.

b. Staff Communications Material Systems Responsibility Officer (SCMSRO). The Head, Security Programs and Information Management Branch (ARS) by the direction of the CO, has the responsibilities and duties that are applicable to the CO unless otherwise indicated.

c. EKMS Manager. An individual designated in writing by the CO to manage COMSEC material issued to the EKMS account. The EKMS manager is the CO's primary advisor on matters concerning the security and handling of COMSEC material, associated records, reports, and audits.

d. Alternate EKMS Manager. The individual designated in writing by the CO/SCMSRO responsible for assisting the EKMS Manager in the performance of their duties and assuming the duties of the EKMS Manager in their absence.

e. Local Element (LE). LEs are separate staff agencies, activities, or commands, internal or external to the parent COMSEC account that requires COMSEC material. LE's receive their COMSEC material from their parent EKMS account. LE Executive Assistants (EA) and COs (Henderson Hall Battalion, Marine Barracks Washington (MBW), Marine Corps Information Operations Center (MCIOC), and/or other command under Letter of Agreement) are ultimately responsible for the proper account management, which includes safeguarding, accounting, handling and disposition of COMSEC material. In addition, LEs must comply with Navy/Marine Corps policies.

f. Primary Local Element Control Officer (LECO)/Security Coordinator. The Security Coordinator/LECO is designated in writing by the staff agency, activities' EA or commands' CO [enclosure (1)] receiving EKMS services and COMSEC material from HQMC (ARS). HQMC (ARS) CO/SCMSRO will appoint the Security Coordinator/LECO [enclosure (2)]. The LECO is responsible to the EKMS Manager for the administration, accounting, handling, and destruction of COMSEC material within their respective accounts. If a LECO is not assigned, the Security Coordinator is responsible to execute the duties below. Appointment letters are valid for two (2) years, upon change of command or upon relief of duty or PCS.

(1) Provide the Basic COMSEC User training (PowerPoint format) and execute the SD Form 572 [enclosure (3)] for all individuals who require access to COMSEC material and equipment.

AMD 1

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

(2) Execute an authorization to draw COMSEC material [enclosure (4)] for all individuals that are required to receive COMSEC material within the authorized holding space of HQMC and must be signed by staff agency, activity or command's CO or EA.

(3) Maintain an inventory listing of all CMS distributed material issued into their custody.

(4) Ensure that all CMS equipment is properly safeguarded in the assigned spaces. If CMS equipment is to be relocated for any reason, the EKMS Manager must be notified and approval provided prior to any move taking place.

(5) Perform all page checks of COMSEC related publications as required.

(6) Ensure that all CMS publications, keying material (Keymat), and any other associated materials are stored in their assigned security container when not in use.

(7) Assist in taking inventories required by the EKMS Manager. Staff agencies, activity or commands issued electronic encryption key via Simple Key Loaders (SKL), are required to turn in the SKL during the first five (5) days of the current month for SKL audits. Failure to turn in the SKL within the prescribed period is considered a NON-Reportable PDS, signed by the command's CO or EA.

(8) Ensure that all CMS distributed material is turned into the EKMS Manager for disposition when no longer needed. Users with assigned COMSEC gear that are no longer attached (PCS, retirement, etc.) must turn in the equipment to the LECO/Security coordinator. This equipment will be returned to the EKMS Manager for re-issue or final disposition.

(9) Conduct local destruction as required per this SOP and forward the documentation (SF-153 or CMS 25) to the EKMS Manager. Staff agencies, activities or commands issued electronic encryption key via SKL, must provide records of loading the electronic key, zeroization/destruction of key via the Modern Key Tracker [enclosure (5)].

(10) Keep the EKMS Manager informed of your impending personnel transfer, retirement, extended leave, or temporary duty assignment. LECO/Security coordinators are encouraged to have an "EKMS/COMSEC Turnover and Desktop Procedures" binder to assist them in their duties.

(11) Ensure that no changes are made to CMS distributed material list unless directed by the EKMS Manager.

(12) Comply with the provisions of this SOP, reference (a), and all written and oral guidance provided by the EKMS Manager.

(13) Authorize access to COMSEC material to only those personnel authorized access by the EKMS Manager.

(14) Maintain the COMSEC Inventory of material for your LE Account, CMS Correspondence File, Message File, CMS Directive File, training documents/logs, and Emergency Action Plan (EAP). Retention period for the LE administrative files are one (1) year from last entry or disposition.

(15) Conduct annual EAP training and document all COMSEC training for your agency, activity or command. A log or email record of training is

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND
DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

required and must list date training was held and attendees. This log is an inspectable item.

(16) LECO/Security coordinators both Primary and Alternate are required to attend initial and refresher COMSEC training annually. Copies for this training will be maintained.

(17) LECO/Security coordinators are required to conduct in conjunction with the LE's CO or Executive Officer (XO) a quarterly (starting January of each calendar year) CO Spot Check using applicable TABS N, O, [reference (f)]. The spot check must be signed by the CO, XO or EA in addition to the LECO/Security coordinator. A copy of the spot checks will be sent to the HQMC EKMS Managers.

g. Alternate Local Element Control Officer. The Alternate LECO is designated in writing by the staff agency, activity or command [enclosure (1)], and then the CO/SCMSRO will appoint him/her as the Alternate LECO [enclosure (2)]. The Alternate LECO assists the Primary LECO with the performance of his/her COMSEC duties. The Alternate LECO may assume the duties of the Primary LECO in his/her absence and is equally responsible for the COMSEC material and EKMS procedures and policies.

h. Account Clerk. An individual designated in writing by the SCMSRO who assists the EKMS Manager and Alternate with routine administrative account matters.

i. CMS User. An individual responsible for the proper security, control, accountability, and disposition of the COMSEC material placed in their charge. CMS User is also referred to as a LE entity. Users are required to take the initial Basic COMSEC User training, continued by mandatory annual training. The user must have an approved/signed SD form 572 prior to handling COMSEC material.

AMD 1

6. Access Requirements

a. Only those individuals who have a "need to know", possess the appropriate security clearance, have been designated in writing, and trained shall be granted access to CMS distributed material. The EKMS Manager and LECO shall maintain enclosure (3) for all personnel authorized access to COMSEC materials. CMS users must execute enclosure (3) certifying that they have read and thoroughly understand this directive. Note: Prior to signing enclosure (3), contractor personnel must be briefed and have been granted COMSEC access in accordance with reference (b). Under no circumstances will contractor personnel be granted access to any COMSEC material or equipment without the express consent of the EKMS Manager.

b. Each CMS user LE that is required to receipt for and pick-up COMSEC material from the EKMS Manager, must be appointed in writing by their CO utilizing enclosure (4). This letter should be updated on an annual basis; when a change of authorized users occurs due to extended leave, PCS, retirement, transfer, etc.; and at the direction of the EKMS Manager. This form will be endorsed by each individual requiring receipt for and pick-up privileges to COMSEC material and returned to the EKMS Manager within 48 hours of requiring access.

7. Storage. Storage spaces for CMS distributed material shall provide maximum protection against unauthorized personnel access and material damage or deterioration. Storage spaces shall be secured when not under the direct supervision of appropriately cleared and authorized personnel. If spaces contain Top Secret material, two appropriately cleared and authorized personnel are required to remain with the material at all times. Storage containers and

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

vaults will be approved by the Physical Security Specialist and shall meet the requirements of reference (c).

8. Two Person Integrity (TPI). The sensitivity of COMSEC Keymat necessitates additional security measures including TPI for Top Secret Keymat, which does not permit lone access.

a. TPI is maintained by a two-lock system. Each lock has its own combination and access list. To access the Top Secret material, two individuals must remain present while the Top Secret material is exposed to prevent a single individual from gaining lone access.

b. CMS users who use Top Secret CMS material will develop two teams for each container storing Top Secret material; one team is labeled alpha and has access to the alpha lock, while the other is bravo with access to the bravo lock. Each team will have a leader and at least one backup. NO person, to include the leader may possess the combinations to both the alpha and bravo locks simultaneously. The leader has the responsibility for ensuring back up access to meet destruction deadlines when the leader is absent.

c. TPI applies to all Top Secret Keymat and Top Secret electronic key stored in a fill device; and unloaded fill devices in an operational communication environment which contain Top Secret keyed crypto-equipment from which key may be extracted. If the equipment itself does not permit extraction of loaded keys or if equipment key ports are protected against unauthorized key extraction using an approved TPI locking device, the unloaded fill devices need not be afforded TPI handling and may be stored under single-lock protection. Simple Key Loaders (SKLs) with Top Secret Keymat will be locked in a TPI safe as long as the Crypto Ignition Key (CIK) is inserted. If the CIK is removed, the SKL and the CIK must be stored in separate locations. The SKL then becomes CCI but no longer requires being stored in a TPI safe. Safeguard and accountability of CCI material still applies.

9. Operational Configuration. COMSEC equipment installed in an operational configuration must meet the storage requirements of paragraph 7 above. Equipment installed for use on circuits which operate only when the area is occupied, and therefore, is zeroized at the close of the working day, requires no additional protection. If the equipment is keyed with a Top Secret key and the key can be extracted from the equipment, the locking devices must be installed to ensure TPI is maintained for the key. In addition, if keyed equipment is to be operated in a "keyed unattended mode" the equipment must be secured to the equipment rack, or an approved intrusion detection system (IDS).

10. Courier Responsibilities

a. Continental U.S. (CONUS) and Outside Continental U.S. (OCONUS) couriers must be authorized in writing and adhere to the Authorization to Hand-carry Classified Material and Communications Security (COMSEC) Equipment and Material [enclosure (6)], and maintain a courier card when traveling with COMSEC material and equipment.

b. Couriers traveling OCONUS (foreign travel) must be authorized in writing by the HQMC Security Manager and adhere to paragraph (a) above. It is mandatory that two couriers be available to share and maintain constant personal custody of all Keymat and equipment. If couriers are required to utilize secure mobile devices, Security Note 06-11 [reference (d)] must be read and adhered to. In addition, couriers must ensure they have the telephone number of the nearest U.S. Embassy or Consulate for every country that the aircraft is scheduled to fly through/into in order to store the COMSEC material as may be necessary/required.

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND
DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

11. Combination, PIN and Password Changes

a. Combinations of containers used to store CMS distributed material shall be changed:

(1) When the lock is initially placed in use. The manufacturer preset combination may not be used.

(2) Whenever a person having knowledge of the combination is transferred or no longer requires access.

(3) Whenever the combination becomes known, or is suspected to have become known, to an unauthorized person.

(4) Every two (2) years. The 24-month period will run from any combination change executed for any reason.

b. After changing the combination to a security container or lock that protects CMS material, the following steps must be taken to protect the combination (and the contents within) from possible compromise:

(1) Fill out a Security Container Information (SF 700).

(2) Part 1 of SF 700 will be inserted into an envelope marked "PII information enclosed". Affix Part 1 of SF 700 sealed in envelope on the inside of the container/vault door near the lock.

(3) Record the new combination on Part 2A of SF 700, fold it in thirds, and then wrap it in aluminum foil. Insert Part 2A into Part 2 of SF 700 and seal. Sign your name(s) along the principal seam, and cover with transparent tape. See enclosure (11) for SF-700 label requirement.

AMD 1

(4) Laminate the SF 700 in plastic.

(5) Turn the sealed combination into the EKMS Manager or remote location within their staff agency, activity or command for storing in a centrally located container for use in an emergency.

c. Access to combinations

(1) Knowledge of the combination to the EKMS Manager's vault and safes shall be limited to the primary and alternate EKMS Managers. Knowledge of combinations to safes and vaults containing CMS distributed material held by Local Elements will be limited to personnel on the COMSEC Access List with an appropriate security clearance and the need to know.

(2) When a TPI locking system is required for security containers, each combination must be maintained in a separate SF 700 form. One SF 700 Form must be marked alpha and the other SF 700 Form must be marked bravo.

12. Reproduction of CMS Material. CMS distributed material shall not be reproduced. Unauthorized reproduction of CMS distributed material may result in criminal proceedings being initiated. Additional copies of CMS material must be requested from the EKMS Manager in advance of the required date.

13. Displaying, Viewing, and Publicly Releasing COMSEC Material and Information

a. Open public display of U.S. Government or foreign government COMSEC material and information at non-governmental symposia, meetings, open houses, or for other non-official purposes is prohibited.

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

(1) This includes discussion, publication, or presentation for other than official purposes.

(2) Photographs, drawings, or descriptive information for press release or private use is prohibited. No external viewing or other exposure, which might afford opportunity for tampering or internal examination, is permitted.

(3) Exterior photographs of COMSEC equipment used for staff agency, activity or command training need not be marked "FOR OFFICIAL USE ONLY".

14. Request for COMSEC Equipment. Requests by LEs for additional COMSEC equipment [including Secure Telephone Equipment (STE)] must be submitted to the "SMB HQMC COMSEC" organizational mailbox, via NIPR using the Security Services Form, [enclosure (7)]. If equipment is available, this request will be filled from existing stock. Equipment not available from existing inventory will be requested from Marine Corps Systems Command. Enclosure (7) must contain the following information:

a. Short title or nomenclature of equipment requested.

b. Date equipment or material required.

c. Desired location of end-crypto unit or STE. [If this is a residential STE request, include Letter of Request for Residential Secure Telephone Equipment [enclosure (8)] with your request.

d. For new Keymat (allow 30 days for production):

(1) Short title and classification of requested Keymat.

(2) Controlling Authority of the requested Keymat (if known).

(3) Equipment material will be used with.

(4) Number of copies of Keymat required.

(5) Type of usage (operational/test/maintenance).

e. Justification for the requirement of equipment and/or Keymat.

15. Modification to Equipment. Modifications to COMSEC equipment will be with modification kits distributed through the COMSEC material system only. The EKMS Manager will coordinate installation of modification kits. Security Agency (NSA) approved software upgrades to COMSEC equipment will be done only and upon receipt of official message from the Department of the Navy, HQMC C4 and Naval Communications Security (NCMS). Equipment upgrades will be reported by equipment short title (ea. KG175D), serial number and unit name to the EKMS Manager via NIPR email. Download of software is restricted to and will be accomplished via NIPR on the Naval Crypto Products & Services website:

<https://infosec.navy.mil/crypto/index.jsp?topic=ine>

No modification/alteration shall be made to COMSEC equipment without prior official approval by the National Security Agency (NSA). Only technicians certified to work on specific types of equipment will install modification kits. Training requirements to be certified in COMSEC equipment maintenance is covered by reference (d).

16. COMSEC Material Transactions. Under no circumstances shall LEs transfer or temporarily loan CMS distributed material. This restriction also applies to the transfer of material between LEs within HQMC. All requests for the

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND
DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

transfer of COMSEC material and equipment must be approved by and handled through the EKMS Manager. All transactions (destructions, receipts and returns) will be effected via the COMSEC Material Report (SF-153) or equivalent. Under no circumstances shall COMSEC material be removed from the current location without written authorization from the EKMS Manager.

17. Issuing of Keying Material (Keymat) to Local Elements. The EKMS Manager will issue Keymat to LEs no more than 30 days in advance of the effective date of the Keymat. Material will be issued using a SF 153.

18. Protection of Keymat. During transportation from the EKMS Manager to the LE location, all material will be double-wrapped and accompanied at all times by two persons. Upon arrival at the LE location, the short title will be added to the LE inventory listing. If it is Top Secret material, then secure material using TPI controls.

19. Keymat Handling Errors. The primary cause of errors in COMSEC key handling is the failure to follow established procedures. Requiring TPI when handling Keymat should eliminate most errors. All errors in Keymat handling must be reported to the EKMS Manager for investigation and completion of any necessary action in accordance with reference (a), chapter 9. Some of the common errors are:

a. Premature Loading of Keymat. When loading Keymat ensure the effective segment is highlighted within your Simple Key Loader (SKL) or Data Transfer Device (DTD). Full attention must be given and no interruptions should be permitted. In the unlikely event of premature loading of a segment, it is mandatory to document the time and date of the premature load, the personnel involved, and the reason for premature loading. This information will be immediately reported to the EKMS Manager.

b. Premature Destruction of Keymat. Destruction of Keymat requires full compliance with established guidelines. In the unlikely event of premature destruction of effective Keymat, the EKMS Manager must be notified immediately.

c. Attempt to Load Wrong Keymat. Attempting to load the improper Keymat for a circuit or for a type of equipment is a reportable COMSEC incident in accordance with reference (a), chapter 9.

20. Local Element Destruction of COMSEC Material

a. Personnel Requirements. Destruction of superseded COMSEC material will always be destroyed by two properly cleared and authorized individuals. The two individuals conducting the destruction of COMSEC material must not complete (i.e. sign and date) destruction documents until after the material has actually been destroyed. Therefore, two individuals conducting the destruction must personally witness the complete destruction of the material in accordance with reference (a), chapter 7.

b. Destruction Methods. Destruction methods and required records are outlined in reference (a), paragraph 540. Placing COMSEC material in a burn bag does not constitute a complete destruction. A complete destruction is destruction by burning, shredding, electronic, or other authorized means to make reproduction impossible.

c. Destruction of Electronic Key. Electronic key issued to an SKL or DTD are deleted after supersession date and after loading into equipment. SKL and DTD audit trail reviews will serve to verify destruction of this key as per reference (a) in addition to Modern Key Tracker (MKT) form [enclosure (5)]. Monthly SKL/DTD audit trails reviews must be accomplished by the EKMS Manager to confirm destruction or document any anomalies. In the event of SKL or DTD

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND
DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

battery failure the electronic key is zeroized. The LE is required to submit a signed CMS25 or MKT Form on all zeroized key and deliver the form to the EKMS Manager. If electronic key is zeroized due to operator error, a NON-Reportable PDS must be submitted with corrective actions to help prevent this from happening again. The NON-Reportable PDS will be signed by the CO, XO, or EA only. A copy will be routed to the HQMC SCMSRO via HQMC EKMS Manager for information and the original kept in the EKMS administrative file for record.

d. Routine Destruction of Operational Keymat. Per reference (a), paragraph 540e, destroy electronic key immediately after use or as soon as possible after it has been superseded or has otherwise served its intended purpose, but always within 12 hours after supersession. Late destruction is a COMSEC incident. Exceptions to this destruction standard is as follows:

AMD 1

(1) In the case of an extended holiday period (over 72 hours) or when special circumstances prevent compliance with the 12-hour standard (e.g., destruction facility or operational spaces not manned, etc.) destruction may be extended until the next duty day. In such cases, material must be destroyed as soon as possible after reporting for duty.

(2) Keymat packaged in canisters containing multiple copies of each segment (e.g., 1/01, 1/02, 1/03, etc.). Retain the last copy of each effective segment until the cryptoperiod expires, then destroy within 12 hours. Destroy all preceding copies of the still effective segment immediately after use.

(3) Material involved in an investigation, in these cases, specific instructions to retain the material beyond the supersession date will be provided via Naval message by Naval Communications Material System Command, code: N5, or the Director of the National Security Agency (NSA), code: I9123.

21. Emergency Supersession of Keymat. Destroy as soon as possible and always within 12 hours of receipt of emergency supersession notification. The only exceptions are addressed in paragraph 20d(1).

22. Destruction of COMSEC Equipment. Destruction of COMSEC equipment is not authorized. Broken or otherwise inoperable equipment will be returned to the EKMS Manager for repair or final disposition.

23. Reporting Destructions. Report destruction of Keymat to the EKMS Manager via the one-time "Keymat Destruction Report" (CMS 25). All destruction reports must be returned to the EKMS Manager no longer than 48 hours after destruction unless otherwise directed by the EKMS Manager. Under no circumstances destroy COMSEC material prior to the supersession date unless directed.

24. COMSEC Incidents. All persons who control or use COMSEC material are responsible for immediately identifying COMSEC incidents and promptly reporting them to the EKMS Manager. Reportable incidents include:

a. Cryptographic Incidents. Examples of cryptographic incidents are:

(1) Use of COMSEC Keymat that is compromised, superseded, defective, previously used (and not authorized for reuse), or incorrectly applied; such as:

(a) Use of Keymat that was produced without the authorization of the NSA, i.e., homemade maintenance, Data Encryption Standard key, or homemade codes.

(b) Use, without the authorization of the NSA, of any Keymat for other than its intended purpose.

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

(c) Unauthorized extension of crypto period.

(2) Use of COMSEC equipment having defective cryptographic logic circuitry, or use of an unapproved operating procedure; such as:

(a) Plaintext transmission resulting from a COMSEC equipment failure or malfunction.

(b) Any transmission during a failure, or after an uncorrected failure that may cause improper operation of COMSEC equipment.

(c) Operational use of equipment without completion of required alarm check test or after failure of required alarm check test.

(3) Use of any COMSEC equipment or device that has not been approved by the NSA.

(4) Discussions via non-secure telecommunications of the details of a COMSEC equipment failure or malfunction.

(5) Any other occurrence that may jeopardize the crypto security of a COMSEC system.

b. Personnel Incidents. Example of personnel incidents are:

(1) Known or suspected defection.

(2) Known or suspected espionage.

(3) Capture by an enemy of persons who have detailed knowledge of cryptographic logic or uncontrolled access to Keymat.

(4) Unauthorized disclosure of information concerning COMSEC material.

(5) Attempts by unauthorized persons to affect such disclosure.

c. Physical COMSEC Material Incidents. Examples of physical incidents are:

(1) The physical loss of COMSEC material includes whole editions as well as classified portions of pages from a maintenance manual, keytape segment, and electronic key. If a record of destruction is required but is not available, the material must be considered lost.

(2) Unauthorized access to COMSEC material by persons inappropriately cleared.

(3) COMSEC material discovered outside of required accountability or physical control; e.g.

(a) Material reflected on a destruction report as having been destroyed and witnessed, but found not to have been destroyed.

(b) Material left unsecured or unattended where unauthorized persons could have had access.

(c) Failure to maintain required TPI for Top Secret Keymat, except where a waiver has been granted.

(4) COMSEC material improperly packaged or shipped.

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

- (5) COMSEC material received with a damaged inner wrapper.
 - (6) Destruction of COMSEC material by other than authorized means.
 - (7) COMSEC material not completely destroyed and left unattended.
 - (8) Actual, or attempted unauthorized maintenance (including maintenance by unqualified personnel), or use of a maintenance procedure that deviates from established standards.
 - (9) Tampering with, or penetration of, a cryptosystem. For example:
 - (a) COMSEC material received in a protective packaging (KSV-21 card, KSD-64, etc.) which shows evidence of tampering.
 - (b) Unexplained (undocumented) removal of Keymat from its protective technology.
 - (c) Known or suspected tampering with or unauthorized modification of COMSEC equipment.
 - (d) Discovery of clandestine electronic surveillance or recording device in or near a COMSEC facility.
 - (e) Activation of the anti-tamper mechanism on, or unexplained zeroization of COMSEC equipment when other indications of unauthorized access or penetration are present.
 - (10) Unauthorized copying, reproduction, or photographing of COMSEC material.
 - (11) Deliberate falsification of COMSEC records.
 - (12) Any other incident that may jeopardize the physical security of COMSEC material.
 - (13) Failure to review audit trail data and maintain an audit review log for equipment with audit capability (e.g., DTD, SKL, TKL, etc...) which have been/are initialized, storing key or issued to an LE since the previous audit trail review was conducted, per the requirements outlined in the specific cryptosystem doctrine. For exceptions to the audit review policy refer to reference (a), see Annex Z, paragraph 17.c (note 3), and Annex AF, paragraph 9.b (note 3).
25. COMSEC Incident Investigations and Reports. Upon report of a possible COMSEC incident, the EKMS Manager will immediately conduct a preliminary investigation. In the event of a confirmed incident the EKMS Manager will immediately report the incident and the result of his preliminary investigation to the CO/SCMSRO, who will appoint an investigating officer to conduct a thorough and in-depth investigation per reference (a). COMSEC incident reports will be submitted in accordance with the stated reference. Initial reports of COMSEC incidents must be submitted within 24 hours after discovery in most cases but no longer than 72 hours in any case.
26. Practices Dangerous to Security (PDS). PDSs are practices which, although not reportable to NSA, have the potential to jeopardize the security of COMSEC material if allowed to perpetuate. All PDSs must be reported to the EKMS Manager, who will investigate and prepare any required reports. PDSs are identified as:

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

- a. Improperly completed accounting reports (i.e., unauthorized signatures, missing signatures, incomplete short title information).
- b. Physical COMSEC Keymat transferred to another COMSEC account with status marking intact.
- c. COMSEC Keymat, publications, or equipment not listed on account, External LE, or Internal LE inventories.
- d. Issue of paper-based or electronic form Keymat, without authorization, to External LE or Internal LE more than 30 days before effective date.
- e. Premature or out-of-sequence use of Keymat before its effective date, as long as the material was not reused. A report must be submitted to the Controlling Authority for the Keymat.
- f. Unauthorized (premature) destruction of COMSEC material as long as the destruction was properly documented. If Keymat destroyed without authorization was also used before its scheduled implementation date it must be reported as a COMSEC incident.
- g. ~~Late destruction of COMSEC material (not within the specified time period).~~
- h. Failure to zeroize a fill device within the required time frame.
- i. Removing Keymat from its protective packaging prior to effective date without authorization, as long as the removal was documented and there was no reason to suspect espionage.
- j. Receipt of a package with a damaged outer wrapper, but an intact inner wrapper.
- k. Activation of the anti-tamper mechanism on, or unexplained zeroization of COMSEC equipment, as long as no other indications of unauthorized access or penetration was present.
- l. Premature or out-of-sequence use of Keymat before its effective date, as long as the material was not reused. Premature use is defined as an on-the-air attempt to establish communications/transmit data. If material prematurely used is reused without consent of the EKMS Manager it must be reported as a cryptographic incident.

AMD 1

27. Inventory Policy. The EKMS Manager may direct or conduct inventories at any time. Two semi-annual mandatory inventories are held in Jan/Feb and Jul/Aug timeframe. When so directed, the Security Coordinator/LECO will accompany the EKMS Manager to visually verify the short title, edition, and accounting number of the COMSEC materials consigned to them on local custody. Upon the conclusion of the inventory the Security Coordinator/LECO shall sign receipt for the results of this inventory via an SF 153 inventory report. It is important that the equipment held at approved residences is accessible during the inventory. Access to these residences will be coordinated with LECO/Security coordinators prior to inventory.

28. Secure Telephone Equipment (STE). Reference (a), Annex AD, promulgates regulations and guidance for issuing, accounting, handling, and safeguarding of these products. These features allow the end user to access the secure mode of the instrument via a KSV-21 card. Protections of these COMSEC products are paramount. The following information provides basic security policy for the protection of these products:

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

a. A security clearance equal to the highest level of Keymat loaded into the terminal is required for access. Keyed is defined as "operational key filled into the device". Whenever persons in an area are not cleared to the level of the keyed device, it must be under the operational control and within view of at least one appropriately cleared, authorized person.

b. A security clearance is not required for access to unkeyed terminals. However, access must be restricted to U.S. Citizens whose duties require such access. Unkeyed equipment must be protected in a manner that is sufficient to preclude any reasonable chance of theft, sabotage, or tampering. An unkeyed terminal may be used for unclassified and non-sensitive calls by persons who meet access requirements.

c. When authorized persons are not present, the KSV-21 card must be removed from the terminal and properly protected. Regardless of approved "OPEN STORAGE" location, at the end of the working day the KSV-21 card must be secured in a locked drawer or safe. Only exception to this procedure: RSAC and COOP locations manned 24/7. A local watch-to-watch inventory of the cards must be kept. Authorized persons must retain these devices, and they must protect the device as valuable personal property.

d. Terminals may be installed in a private residence based on operational requirements authorized by the individual's staff agency, activity or commands' CO or EA with final approval is given by the EKMS Manager. All residential installations are a privilege and may be suspended or revoked at any time without notice. The following security requirements must be followed:

(1) A formal written request by the staff agency, enclosure (8), must be provided to the EKMS Manager before a Residential STE can be issued.

(2) The terminal must be used only by the person for whom it was installed. Prior to issuing the STE phone and card a Physical Security Survey (PSS) and certification is required of the residence. All security requirements should be observed for preventing unauthorized access to the keyed terminals, to classified, and sensitive unclassified U.S. Government information.

(3) The KSV-21 card must be removed from the terminal following each use and kept in the personal possession of the user or stored in a security container approved for the classification level of the terminal's key.

(4) The KSV-21 card and/or terminal must be returned when requested by the EKMS Manager for inventory or regularly scheduled maintenance. Failure to return the items when requested will automatically revoke this privilege.

(5) Prior to personnel reassignment, retirement or transfer, the terminal and KSV-21 card must be returned to the EKMS Manager via the Local Element's LECO/Security coordinator along with a copy of the CMS Acknowledgment Form annotating change. Failure to return this equipment is equal to theft of government property and a COMSEC incident (KSV-21 card only).

e. Immediately report the loss of a STE terminal KSV-21 card to the EKMS Manager.

f. When communicating in the secure mode, ensure your location will not result in the compromise of classified discussions by eavesdropping.

g. STE terminals are required to be rekeyed quarterly (every 3 months) by following STE rekey procedures found in the HQMC (ARS) website link, <https://ppicss.hqi.usmc.mil/IPCPSP/Home/policyDocuments.aspx#comSec> (select: STE Rekey Procedures (DOC). Note: must have a PPICSS account to access file.

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND
DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

h. All requests for secure terminals must be sent to the EKMS Manager via the LECO or agency Security Coordinator. Furthermore, all personnel that have access to the terminal (regardless of use) must complete enclosure (2).

29. Iridium Secure Module (ISM). Reference (a), Annex AD, promulgates regulations and guidance for the handling and safeguarding of these products. The ISM/Iridium satellite telephone is a handheld Future Narrow Band Digital Terminal compatible device designed to provide users worldwide secure voice connectivity in mobile environments. The secure voice is activated by entering a personal identification number (PIN). The following information contains basic security policy and procedures for the protection of the ISM:

a. The ISM is a controlled cryptographic item when the ISM PIN code has not been entered, the PIN remains separate from the phone, or the ISM is not keyed.

b. When the ISM PIN is entered, the device must be protected to the classification level of the key it contains per reference (a), Annex AD.

c. The ISM user must maintain continuous physical control of the device or keep it stored in a security container that will minimize the possibility of loss, theft, unauthorized use, or tampering.

d. When communicating at a secure/sensitive level and/or entering a PIN code, ensure that your environment will not result in compromise of classified/sensitive discussions.

30. Secure Mobile Environment/Portable Electronic Device (SME/PED). Per reference (f), there are significant security concerns when using SME/PEDs. SME/PEDs are an extension of our network however they are not constrained to USMC physical boundaries at all times. Due to their mobile nature, it is critical that proper controls and procedures are in place. For the purpose of this SOP, Zone 3 SME/PEDs are discussed. Further guidance on the different PED Zone requirements, specifically on Zone 3, are described in reference (g).

AMD 1

a. Zone 3. Any PED which processes, stores, or transmits DoD/Marine Corps information which is classified at the SECRET level (i.e., SME/PED).

b. Ownership. Zone 3 PEDs will be government owned and operated, and require approval prior to use by the Authorizing Official (AO)/Designation Accrediting Authority (DAA).

c. User Agreements. Zone 3 PED users will sign a DoD User Agreement and a CMS Acknowledgment Form after completing the mandatory COMSEC User and SME/PED User training. This agreement will include additional terms that define the AO/DAA authorized tasks for the PED and the authorized PED applications.

d. Passwords. Zone 3 PEDs will be password protected. At a minimum, passwords will contain 15 characters (minimum 2 of 2 special characters, 2 numbers, and 2 upper case letters).

e. Tethering and Hot Docking. Tethering Zone 3 PEDs will be completed via a wired interface only. All wireless connections must be AO/DAA approved.

f. Removable Storage Media. Zone 3 PEDs with removable storage media capabilities will be AO/DAA approved for use on a case-by-case basis.

g. PED Screen Display. Due to the nature of Zone 3 PEDs, users will constantly be aware of their surroundings and ensure proper operational

Subj: STANDING OPERATING PROCEDURES FOR THE HANDLING, ACCOUNTABILITY AND
DISPOSITION OF COMMUNICATIONS SECURITY MATERIAL

security at all times. In addition, privacy screens are encouraged for all Zone 3 PEDS, if available.

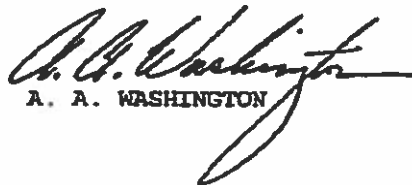
h. Traveling with PEDs. Complete details for Zone 3 PEDs for traveling requirements are on page 26 of reference (g).

AMD 1

31. Other Equipment Rekey Requirements. All other secure products (KG 175 series, SWT, SME/PED, GSM, OMNI, TALON, KIV 7 series and KG 245 series) have Keymat expiration dates. Users will be informed of the Keymat expiration date when the equipment and Keymat is issued and/or any change to expiration information is available via separate correspondence. Depending on the equipment it may require a yearly rekey or it can be rekeyed via secure rekey call procedures. It is important to understand that if the expiration date has passed, this will prevent the device from accessing the secure mode and/or transmit information with expired key [this is a cryptographic incident as per reference (a), chapter 9)].

32. Emergency Action and Emergency Destruction Plans. All LECOs/Security Coordinators shall thoroughly familiarize themselves with the provisions set forth in the basic Emergency Action Plan (EAP) and Emergency Destruction Plan (EDP) for Communication Security Material [enclosure (9)] and develop a detailed EAP/EDP for all CMS materials under their control. EAP/EDP training is required to be held annually "calendar year" and documented. All personnel in addition to the LECO/Security Coordinator should be familiar with the EAP/EDP. In the event of an emergency and destruction is ordered by the on-site senior officer in charge, the CMS user shall destroy CMS distributed material by an authorized technique per EKMS 1 and immediately report the destruction to the LECO/Security Coordinator. The LECO/Security Coordinator will send a detailed report to the HQMC EKMS Manager outlining when, where, and how the event occurred; personnel involved; inventory of COMSEC equipment/material destroyed and on-hand; and type of compromise occurred [see reference (a), chapter 9, paragraph 970]. The EAP/EDP will include destruction plans and incorporate procedures to guarantee emergency destruction under TPI, both of which have authorized access or equal level of clearance to material being destroyed.

33. The purpose of this document is to prepare you as users and LEs to assume your role in the protection of these cryptographic systems. Although not all encompassing, this brief overview covers key points you should be aware of as COMSEC users. If at any time you have questions regarding COMSEC material or equipment, please contact the HQMC EKMS Managers at (703) 614-2305, (703) 693-3135 or (571) 256-8654.


A. A. WASHINGTON

Distribution:

DC PPO
DC C4
DC INTEL
DC P&R
CMC COMMTEAM
CO, MarBks
HQMC, ARI