

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.

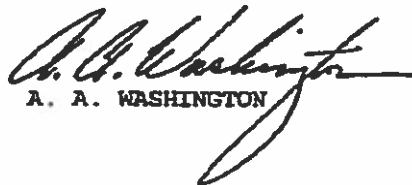
h. Traveling with PEDs. Complete details for Zone 3 PEDs for traveling requirements are on page 26 of reference (g).

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

(COMMAND LETTER HEAD)

5510
CODE
Date

From: Deputy Commandant/Director, Staff Agency/Activity
To: Staff Sergeant Ira M. Gungee, EDIPI/MOS, USMC or USMCR

Subj: NOMINATION AS STAFF AGENCY/ACTIVITY SECURITY COORDINATOR AND LOCAL
ELEMENT CONTROL OFFICER

Ref: (a) SECNAV M-5510.30
(b) EKMS 1 (SERIES)
(c) HQMC IPSP SOP
(d) SECNAV M-5510.36
(e) HQMC ARS EKMS SOP

1. In accordance with reference (a), you are hereby nominated as the Staff Agency/Activity Security Coordinator and per reference (b) you may be required the additional duties of (Primary or Alternate) Local Element Control Officer (LECO). You will be notified of any change in this nomination, when necessary.
2. You are directed as the Security Coordinator to familiarize yourself with the provisions of references (a), (c), and (d).
3. As LECO you are directed to familiarize yourself with references (b), and (e). (Only if assigned as LECO)
4. By return endorsement you will indicate that you have assumed the duties as the Security Coordinator and Local Element Control Officer (If assigned as LECO).

Signature of Deputy Commandant/Director

Date

FIRST ENDORSEMENT

From: Individual Nominated
To: Deputy Commandant/Director, Staff Agency/Activity

1. I have assumed the duties as the Security Coordinator and Local Element Control Officer and will familiarize myself with the listed references.

Signature of Appointee

FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES. The use of electronic signatures are acceptable provided all legal requirements (e.g., authenticity, non-repudiation, verification and records management/storage are met. Legal requirements include but are not limited to 15 U.S.C. 7001, 7006, and 7021.

Enclosure (1)

(COMMAND LETTER HEAD)

5510
ARS
Date

From: Staff Communications Material Systems Responsibility Officer (SCMSRO)
Headquarters, United States Marine Corps
To: Staff Sergeant I. M. Gungee, EDIPI/MOS, USMC or USMCR (Civilians
require full name only)

Subj: PRIMARY/ALTERNATE LOCAL ELEMENT CONTROL OFFICER LETTER OF APPOINTMENT

Ref: (a) EKMS 1 (series)
(b) Standing Operating Procedures (SOP) for the Handling, Accountability,
and Disposition of Communications Material Systems (CMS)
(c) Nomination letter received from your command

1. Per the references, you are hereby appointed as the Staff Agency/Activity Security Coordinator and Primary/Alternate Local Element Control Officer (LECO) for the (agency/section).

2. EKMS Account Number: 169078

3. You will familiarize yourself with the information contained in the references.

4. You are responsible to ensure you have completed all requirements in accordance with reference (b) prior to detachment or reassignment from this headquarters.

5. Per reference (a), local element training is provided on a semi-annual basis. Prior to attending the local element training you will be provided with instructions for the safeguarding, storage, and handling of the Communication Security (COMSEC) material assigned to your agency/activity. The HQMC Electronic Key management System (EKMS) manager, will contact you to schedule this required training.

6. The point of contact for this matter is the EKMS Manager, at (703)614-2305/693-3135.

I. M. SMITH

FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES. The use of electronic signatures are acceptable provided all legal requirements (e.g., authenticity, non-repudiation, verification and records management/storage are met. Legal requirements include but are not limited to 15 U.S.C. 7001, 7006, and 7021.

Enclosure (2)

CRYPTOGRAPHIC ACCESS CERTIFICATION AND TERMINATION**PRIVACY ACT STATEMENT****AUTHORITY:** EO 9397, EO 12333, and EO 12356**PRINCIPAL PURPOSE(S):** To identify the individual when necessary to certify access to classified cryptographic information**ROUTINE USE(S):** None**DISCLOSURE:** Voluntary, however, failure to provide complete information may delay certification and, in some cases prevent original access to classified cryptographic information**INSTRUCTIONS**

Section I of this certification must be executed before an individual may be granted access to classified cryptographic information

Section II will be executed when the individual no longer requires such access

Until cryptographic access is terminated and Section II is completed, the cryptographic access granting official shall maintain the certificate in a legal file system, which will permit expeditious retrieval. Further retention of the certificate will be as specified by the DoD Component record schedules.

SECTION I - AUTHORIZATION FOR ACCESS TO CLASSIFIED CRYPTOGRAPHIC INFORMATION

a. I understand that I am being granted access to classified cryptographic information. I understand that my being granted access to this information involves me in a position of special trust and confidence concerning matters of national security. I hereby acknowledge that I have been briefed concerning my obligations with respect to such access.

b. I understand that safeguarding classified cryptographic information is of the utmost importance and that the loss or compromise of such information could cause serious or exceptionally grave damage to the national security of the United States. I understand that I am obligated to protect classified cryptographic information and I have been instructed in the special nature of this information and the reasons for the protection of such information. I agree to comply with any special instructions, issued by my department or agency regarding unofficial foreign travel or contacts with foreign nationals.

c. I acknowledge that I may be subject to a non-lifestyle, counterintelligence scope polygraph examination to be administered in accordance with DoD Directive 5210.48 and applicable law.

d. I understand fully the information presented during the briefing I have received. I have read this certificate and my questions, if any, have been satisfactorily answered. I acknowledge that the briefing officer has made available to me the provisions of Title 18, United States Code, Sections 641, 793, 794, 798, and 952. I understand that, if I willfully disclose to any unauthorized person any of the U.S. classified cryptographic information to which I might have access, I may be subject to prosecution under the Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States, as appropriate. I understand and accept that unless I am released in writing by an authorized representative of (insert appropriate security office), the terms of this certificate and my obligation to protect all classified cryptographic information to which I may have access, apply during the time of my access and at all times thereafter.

ACCESS GRANTED THIS _____ DAY OF _____, _____.

1. EMPLOYEE

a. SIGNATURE	b. NAME (Last, First Middle Initial)	c. GRADE/RANK/RATING	d. SSN
--------------	--------------------------------------	----------------------	--------

2. ADMINISTERING OFFICIAL

a. SIGNATURE	b. NAME (Last, First Middle Initial)	c. GRADE	d. OFFICIAL POSITION
--------------	--------------------------------------	----------	----------------------

SECTION II - TERMINATION OF ACCESS TO CLASSIFIED CRYPTOGRAPHIC INFORMATION

I am aware that my authorization for access to classified cryptographic information is being withdrawn. I fully appreciate and understand that the preservation of the security of this information is of vital importance to the welfare and defense of the United States. I certify that I will never divulge any classified cryptographic information I acquired, nor discuss with any person any of the classified cryptographic information to which I have had access, unless and until freed from this obligation by unmistakable notice from proper authority. I have read this agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Title 18, United States Code, Sections 641, 793, 794, 798, and 952 and Title 50, United States Code, Section 783(b).

ACCESS WITHDRAWN THIS _____ DAY OF _____, _____.

3. EMPLOYEE

a. SIGNATURE	b. NAME (Last, First Middle Initial)	c. GRADE/RANK/RATING	d. SSN
--------------	--------------------------------------	----------------------	--------

4. ADMINISTERING OFFICIAL

a. SIGNATURE	b. NAME (Last, First Middle Initial)	c. GRADE	d. OFFICIAL POSITION
--------------	--------------------------------------	----------	----------------------

REQUEST FOR AUTHORIZATION TO DRAW COMSEC MATERIAL FORM

From: _____
(Head, Agency, Section, Branch Department)
To: Electronic Key Management Systems Manager, Security Programs and
Information Management Branch (ARSC)
Subj: REQUEST FOR AUTHORIZATION TO DRAW COMSEC MATERIAL FORM
Ref: (a) EKMS 1 (series)
(b) Standing Operating Procedures (SOP) for the Handling,
Accountability and Disposition Of Communications Materials Systems
(CMS)

1. The individuals identified below are authorized to receive COMSEC Material on behalf of Local Element 169078. These appointees are authorized to receive COMSEC material within the authorized holding space of HQMC. As such, these appointees have read and familiarized themselves with the provisions of the references.

NAME	GRADE	EDIP	CLEARANCE	USER SIGNATURE
------	-------	------	-----------	----------------

NAME	GRADE	EDIP	CLEARANCE	USER SIGNATURE
------	-------	------	-----------	----------------

NAME	GRADE	EDIP	CLEARANCE	USER SIGNATURE
------	-------	------	-----------	----------------

AUTHORIZED SIGNATURE AND DATE

Date

From: Electronic Key Management Systems Manager, Security Programs and
Information Management Branch (ARSC)
To: _____

1. Approved/Disapproved.

EKMS Manager Signature

FOR OFFICIAL USE ONLY - PRIVACY SENSITIVE: ANY MISUSE OR UNAUTHORIZED DISCLOSURE MAY RESULT IN BOTH CIVIL AND CRIMINAL PENALTIES. The use of electronic signatures are acceptable provided all legal requirements (e.g., authenticity, non-repudiation, verification and records management/storage are met. Legal requirements include but are not limited to 15 U.S.C 7001, 7006, and 7021.

Enclosure (4) **AMD 1**

USE THE YELLOW SECTION WHEN
DESTROYING KEY FROM EQUIPMENT

 Y/N [illegible]

USE this side AFTER DELETING key from EQP

DATE: _____

PRINT NAME: _____

SIGNATURE: _____

PRINT NAME: _____



CONFIDENTIAL WHEN FILLED IN

AGREEMENT TO HAND-CARRY CLASSIFIED MATERIAL

BASIC POLICY

Individual's hand-carrying classified information or material, either within or outside of a command, must take every precaution to prevent the unauthorized disclosure of the information or material.

HAND-CARRYING WITHIN A COMMAND OR IMMEDIATE ENVIRONS

1. When classified material is being carried within the command or its immediate environs as part of normal duties, an individual must take reasonable precautions to prevent inadvertent disclosure. Reasonable precautions include using a cover sheet or file folder or whatever covering is needed to protect against casual observation of the classified information. The precautions are to be taken whenever material is being moved.
2. When classified material is being carried between buildings (i.e. between the Pentagon and Marine Corps Base Quantico), the classified material will be double-wrapped. Use of large manila envelopes is authorized. A briefcase may be considered as a second layer.
3. When classified material being carried, is actually being transferred to another command, the requirements of SECNAVINST 5510.36 will be followed for wrapping, addressing, receipts, etc.

AUTHORIZATION TO HANDCARRY CLASSIFIED MATERIAL IN A TRAVEL STATUS

4. Because of the inherent security risk, hand-carrying of classified material, while in a travel status, requires approval be granted before travel commences and only when mission essential. Security Managers will authorize hand-carrying only when:
 - a. The classified material is not available at the destination.
 - b. The classified material is needed urgently for a specific official purpose.
 - c. There is specified reason that the material cannot be transmitted by other approved means to the destination in sufficient time for the stated purpose.

Under no circumstances will the hand-carrying of classified material involving overnight stops be authorized, unless a secure storage site at a U.S. Government activity or a cleared contractor facility has been arranged in advance.

PROTECTION DURING HANDCARRYING IN A TRAVEL STATUS

5. Before departure, a traveler authorized to hand-carry classified material will be briefed as follows:
 - a. When carrying keying material and equipment outside the National Capital Region (NCR) it is highly recommended that couriers be available to share and maintain constant personal custody of all keying material and equipment. This is necessary in case of car accidents, restroom break, etc.

b. All classified material must be in your physical possession at all times, unless properly stored at a U.S. Government activity or appropriately cleared contractor facility (Continental U.S. only) is available. Hand-carrying classified material on trips that involve an overnight stopover is not permitted without advance arrangements for proper overnight storage on a government activity or cleared contractor facility. When you surrender any package containing classified material for temporary storage (e.g. overnight or during meals) you must obtain a receipt by an authorized representative of the contractor facility or Government installation accepting responsibility for safeguarding the package.

c. You may not read, study, display, or use classified documents in any manner in a public place.

d. When the classified material is carried in a private, public or government conveyance, you will not store it in any detachable storage compartment such as an automobile luggage rack, aircraft travel pod or drop tank. YOU MAY NOT LEAVE CLASSIFIED MATERIAL UNATTENDED UNDER ANY CIRCUMSTANCES.

e. A list of all classified material carried or escorted by you will be maintained by your command. UPON YOUR RETURN, YOU MUST ACCOUNT FOR ALL CLASSIFIED MATERIAL.

f. Whenever possible you should return the classified material to your command by one of the other approved methods of transmission.

6. Knowing that hand-carrying is generally discouraged, contractors are frequently reluctant to allow visitors to hand-carry classified material back to their duty stations. To resolve this problem, travel orders or visit request to contractor facilities should state whether the visitor is authorized to hand-carry classified material.

**UPON DETACHEMT, PCA, PCS, OR REASSIGNMENT YOU MUST RETURN YOUR COURIER CARD TO ROOM 2A288A (SECURITY PROGRAMS AND INFORMATION MANAGEMENT BRANCH).

AGREEMENT TO HAND-CARRY CLASSIFIED MATERIAL

I _____ HAVE READ AND UNDERSTAND THE PROVISIONS AS STATED IN THE PREVIOUS PAGES:

MEMBER SIGNATURE _____ DATE: _____

WITNESS SIGNATURE _____ DATE: _____



SECURITY SERVICES FORM

DATE REQUESTED: _____

AGENCY/DEPARTMENT REPRESENTATIVE INFORMATION:

NAME: _____ PHONE # _____

OFFICE CODE/ROOM # _____

EXACT LOCATION OF SERVICE REQUESTED _____

TYPE OF SERVICE REQUESTED

COMMUNICATION SECURITY: _____ CRYPTO MATERIAL/KEYING _____ SECURE PRODUCT

REQ/REPAIR _____ INSTALLATION _____ OTHER _____

PHYSICAL SECURITY: _____ LOCKS _____ ALARMS _____ KEY REQUEST _____ COMBO CHANGES

_____ SAFES _____ OFFICE CERTIFICATION _____ OTHER _____

BRIEF DISCRIPTION OF THE SERVICE REQUESTED: _____

ASSIGNED TO: _____ DATE COMPLETED: _____

FOLLOW-UP SERVICE DESCRIPTION/NOTES (IF REQUIRED): _____

CUSTOMER SATISFACTION RATING

1 2 3 4 5 6 7 8 9 10

(1 represents the least satisfied with the level of service provided 10 representing completely satisfied)

CUSTOMER COMMENTS: _____

CUSTOMER SIGNATURE: _____ DATE: _____

(COMMAND LETTER HEAD)

5510
CODE
Date

From: Director or Equivalent, Your Staff Agency
To: Director, Administration and Resource Management Division

Subj: REQUEST FOR RESIDENTIAL SECURE TELEPHONE EQUIPMENT (U//FOUO)

Ref: (a) SOP for the Handling, Accountability and Disposition Of
Communications Material System

1. Per the reference, request approval for the installation of Secure Telephone Equipment (STE) in the residence of (Name of Individual).
2. Provide a sound justification of why secure communications is required on a 24/7 basis, i.e. ensure situational awareness for senior executives, response to classified situations, etc.
3. The KSV-21 cryptocard will either be secured in a GSA approved security container or under the personal control of the authorized individual at all times - assigned personnel have authorization to carry classified.
4. The point of contact in this matter.

SIGNATURE

Copy to: HQMC EKMS Manager (ARS)

Enclosure (8)



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

IN REPLY REFER TO:

5500

ARS

FEB 5 2014

From: Staff Communications Material Systems Responsibility Officer (SCMSRO)
ACCOUNT 169078
To: Distribution List
Subj: EMERGENCY ACTION PLAN FOR COMMUNICATIONS SECURITY MATERIAL
Ref: (a) EKMS 1 (series) ANNEX L
(b) Standing Operating Procedures (SOP) For the Handling,
Accountability and Disposition of Communications
Security Material

1. Purpose. Per the references, this letter prescribes policy and procedures for planning, protecting, and destroying Communication Security Material (CMS) during emergency conditions. This plan shall be incorporated into the Local Element (LE) Communication Security (COMSEC) Emergency Action Plan (EAP).

2. Cancellation. This SOP cancels and supersedes any previous EAP SOP dated prior to Feb 5, 2014.

3. Information. All staff agencies/activities serviced within Headquarters Marine Corps (HQMC) that hold COMSEC or Controlled Cryptographic Item (CCI) material, must prepare emergency action plans for safeguarding such material in the event of an emergency. This letter provides guidance and instruction for all HQMC LEs regarding an EAP and will be incorporated within the existing agency/activity EAP.

4. Guidelines for Minimizing Actions

a. Hold only the minimum amount of COMSEC material at any time [i.e., routine destructions should be conducted as required and excess COMSEC material returned to the Electronic Key Management Systems (EKMS) manager for disposition].

b. COMSEC material should be stored and inventoried in ways that will facilitate emergency evacuation or destruction.

c. Store COMSEC material and CCI equipment to facilitate emergency removal or destruction (e.g., separate COMSEC material from other classified material and segregate COMSEC keying material by status, type and classification).

NOTE: COMSEC material that has been designated for "NATO" use is not exclusively NATO material but is in fact COMSEC material. Consequently, this material need not be separated from other COMSEC material but must be stored and segregated by status and classification.

d. As emergency situations develop, initiate precautionary destruction of all material not immediately needed for continued operational effectiveness. Evacuate all COMSEC material not being destroyed to:

Headquarters Marine Corps
3000 Marine Corps Pentagon
Washington, DC 20350-3000
(Attn: EKMS Manager/Room 2A288A)

Enclosure (9)

Subj: EMERGENCY ACTION PLAN FOR COMMUNICATIONS SECURITY MATERIAL

Except under extraordinary conditions (e.g., an urgent need to restore secure communication after relocation), COMSEC keying material should be destroyed rather than evacuated. After the destruction of material is accomplished notify the EKMS manager to begin resupply planning.

5. Emergency Planning Three categories of COMSEC material that may require destruction in hostile emergencies and only when confirmed enemy action is taking place in the immediate local area of the agency/activity are: COMSEC keying material, COMSEC-related material (e.g., maintenance manuals, operating instructions, and general doctrinal publications), and equipment.

a. Precautionary Destruction When precautionary destruction is necessary, destroy keying material and nonessential manuals in accordance with this plan.

b. Complete Destruction Assign different persons to destroy the material in each category by means of separate destruction facilities, (e.g., Level Three Restricted Areas) and follow the priorities listed herein as incorporated into your EAP.

c. In most instances disaster and events strikes with little or no warning. It is paramount that all personnel who handle COMSEC material are fully aware of the conditions in which material must be either destroyed or evacuated. The following outlines specific conditions that require action in the event an EAP must be implemented:

- (1) Biological/Chemical Threat
- (2) Fire
- (3) Imminent Weather Threat
- (4) Terrorist Activity/Attack Hostile Action

d. The following courses of action are directed pertaining to the specific disaster:

(1) Biological/Chemical Threat. When notified by the EKMS manager or security coordinator that a biological/chemical threat is imminent, execute precautionary destructions in accordance with 5a of this EAP.

(2) Fire. When a fire is detected the following immediate action will be taken:

(a) Take the initial fire fighting measures using available resources if possible AT NO TIME WILL YOU JEOPARDIZE LIFE.

(b) Secure all classified material in proper containers, if possible, otherwise leave classified material inside the space to be consumed by flames rather than subject personnel to the danger of injury or death.

(c) If the situation and safety permits, post a guard at the entrance of your office to direct the fire fighting personnel and to ensure that no classified information is removed.

(d) At all times the EAP and COMSEC Inventory records should be in the LECO/Security coordinator's possession. These records are essential to reconstruct the amount, type, and accountability of all COMSEC material in the event of total destruction or insecurity.

Enclosure (9)

Subj: EMERGENCY ACTION PLAN FOR COMMUNICATIONS SECURITY MATERIAL

(e) After the fire is under control, conduct an inventory of all COMSEC materials and other related items. Conduct a LE inventory and report all findings immediately to the EKMS Manager.

(3) Imminent Weather Threat. If an emergency is created by natural causes (i.e., flood, tornado, etc.) the following procedures will be taken:

(a) Secure COMSEC material only in containers and space approved for their storage. Unless COMSEC material is under the direct control of authorized persons, keep containers and spaces locked.

(b) If at any time severe weather (i.e., floods or tornadoes) may become a factor in damaging COMSEC equipment that is stored in your area; all equipment will be brought to the Headquarters Marine Corps, Security Programs and Information Management Branch (ARS) CMS vault located in room 2A288A at the Pentagon for proper storage. AT NO TIME WILL YOU JEOPARDIZE LIFE.

(4) Terrorist Activity/Attack Hostile Action. When hostile actions occur, it may be assumed that classified material is a target and all efforts must be taken to protect the material from unauthorized disclosure. The following procedures should be carried out until such point as directed by higher authority:

(a) Protecting. When ordered to secure COMSEC material, all material will be properly secured in the HQMC CMS area. If possible, all CMS material will be returned to the ARS CMS Custodian for storage, except material that is required for immediate operational use.

(b) In the event of terrorist attack, all COMSEC equipment will be destroyed to eliminate the possibility of compromise.

e. The three options available in an emergency are securing the material, removing it from the scene of the emergency, or destroying it. If it appears that a condition may be temporary in nature, for example, if it appears that a civil uprising is to be short lived, and your office space is to be only temporarily abandoned, the actions to take could be:

(1) Ensure that all superseded keying material has been destroyed.

(2) Gather up the current and future keying material and take it with you.

(3) Remove classified and CCI elements from crypto-equipment and lock them, along with other classified COMSEC material, in approved storage containers.

(4) Secure the facility and leave.

Note: If it appears that the facility is likely to be overrun or untenable as a direct result of the event, the Emergency Destruction Plan (EDP) should be put into effect.

5. Destructions

a. When directed to implement emergency destructions, all personnel will report immediately to their offices. If sufficient numbers of personnel are not available, ARS will make additional personnel available immediately.

Enclosure (9)

Subj: EMERGENCY ACTION PLAN FOR COMMUNICATIONS SECURITY MATERIAL

b. The EDP is prepared to delineate the procedures to be followed during the destruction process. As personnel arrive to their offices, the senior person present will direct the emergency destruction priorities as indicated on the specific security container. These tasks will be completed as rapidly and thoroughly as possible. Staff agencies are required to designate the destruction priority on each security container containing COMSEC material.

c. The preferred methods of destruction are burning or shredding. Shredding will be restricted to the CMS keying material and classified documents.

d. COMSEC material will be destroyed in the priority sequence established below, with CMS keying material destroyed first. Other material will be destroyed in the same manner as used with CMS keying material.

e. The following list the priority for destruction or evacuation of COMSEC material:

(1) Precautionary Destruction Priority List A:

(a) Superseded keying material and secondary variables.

1. TOP SECRET primary keying material.
2. SECRET, CONFIDENTIAL, and UNCLASSIFIED primary keying material.

(b) Future (reserve on board) keying material for use 1 or 2 months in the future.

(c) Nonessential classified manuals:

1. Maintenance Manuals
2. Operating Manuals
3. Administrative Manuals

(2) Complete Destruction Priority List B:

(a) Keying Material

1. All superseded keying material designated CRYPTO, except tactical operations and authentication codes classified below SECRET.

2. Currently effective keying material designated CRYPTO (including key stored electronically in crypto equipment and fill devices), except unused two-holder keying material and unused one-time pads.

3. TOP SECRET multi-holder (i.e., more than two holders) keying material marked CRYPTO that will become effective within the next 30 days.

4. Superseded tactical operations codes classified below SECRET.

5. SECRET and CONFIDENTIAL multi-holder keying material marked CRYPTO that will become effective within the next 30 days.

Enclosure (9)

Subj: EMERGENCY ACTION PLAN FOR COMMUNICATIONS SECURITY MATERIAL

6. All remaining classified keying material, authentication systems, maintenance, and unused one-time pads.

(b) COMSEC Aids

1 Complete COMSEC equipment maintenance manuals or their sensitive pages. When there is insufficient time to completely destroy these manuals, every reasonable effort must be made to destroy their sensitive pages.

2. National, department, agency, and service general doctrinal guidance publications.

3. Status documents showing the effective dates for COMSEC keying material.

4. Keying material holder lists and directories.

5. Remaining classified pages of maintenance manuals.

6. Classified cryptographic and non-cryptographic operational general publications (e.g., AMSG's and NAG's).

7. Cryptographic Operating Instructions (KAOs).

8. Remaining classified COMSEC documents.

(c) Equipment Make a reasonable effort to evacuate equipment, but the immediate goal is to render them unusable and unserviceable.

1. Zeroize the equipment if the keying element (e.g., KIV 7, STE/KSV-21 card and phone, TACLANE) cannot be physically withdrawn.

2. Remove and destroy readily removable classified elements (e.g., printed-circuit boards).

3. Destroy remaining classified elements.

Note: Unclassified chassis and unclassified elements need not be destroyed.

(3) Complete Destruction Priority List C: In cases where personnel and/or facilities are limited, follow the destruction priority list below:

(a) All superseded and currently effective keying material marked CRYPTO (including key stored electronically in crypto-equipment and fill devices), except tactical operations codes and authentication systems classified below SECRET, unused two-holder keying material, and unused one-time pads.

(b) Superseded tactical operations codes classified below SECRET.

(c) Complete COMSEC equipment maintenance manuals or their sensitive pages.

(d) Classified general COMSEC doctrinal guidance publications.

(e) Classified elements of COMSEC equipment.

Enclosure (9)

Subj: EMERGENCY ACTION PLAN FOR COMMUNICATIONS SECURITY MATERIAL

(f) Remaining COMSEC equipment maintenance manuals and classified operating instructions.

(g) Remaining classified COMSEC material.

(h) Future editions of multi-holder (i.e., more than two holders) keying material and current but unused copies of two-holder keying material.

6. Conducting Emergency Destructions. Any methods approved for routine destruction of classified COMSEC material may be used for emergency destruction. Note: Accurate reporting of information concerning extent of the emergency destruction is second in importance only to the destruction of the material itself.

a. Although the act of emergency destruction of COMSEC material is paramount, all reports (i.e. inventory, destruction, on-hand, etc.) of COMSEC material will be sent to the EKMS manager immediately following the disaster or event. Prepare an inventory of classified materials to be destroyed or evacuated. In the event of actual destruction or evacuation this inventory will serve as a record of destruction or evacuation as required.

b. State in the report the method and extent of the destruction, and any COMSEC material items presumed to have been compromised (e.g., items either not destroyed or not completely destroyed).

c. Names of personnel actually involved in the destruction or evacuation.

7. Designation of Personnel. Local Element Control Officers (LECO) shall designate sufficient personnel to effect the destruction or evacuation of COMSEC material. These designees should be familiar with the provision of this document and reference (a) to effect the destruction or evacuation of COMSEC material within the staff agency/activity.

8. Training. LECO's shall conduct annual exercises to ensure everyone, especially newly assigned personnel who might have to take part in an actual emergency, will be able to carry out their duties. The EKMS manager is required to conduct annual training exercises. Notification of these exercises will be published under separate correspondence within the Local Element and every training must be recorded (log or email) with the date and attendees. The training log is an inspectable item during EKMS inspections.

9. LEs are required to complete the COMSEC portion of the EAP for their respective agencies.


M. M. OLIVER, JR.

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

Enclosure (9)

Sample External Command EKMS Support Request letter

(COMMAND LETTER HEAD)

5500

From: Requesting External Agency, Commanding Officer
To: Staff Communications Material Systems Responsibility Officer (SCMSRO)
Account 169078
Via: (If required)

Subj: REQUEST FOR COMMUNICATIONS SECURITY (COMSEC) SUPPORT

Ref: (a) EKMS 1 (series)

1. (Command/Organization/Unit/Section) located at (geographical location) requests COMSEC material support from Headquarters Marine Corps ARS. The need for COMSEC material is vital to our command's communication needs. On a daily basis this command requires the transmittal of classified, confidential, and sensitive information by different means of communications such as voice, video, and data. By obtaining secure means of communication our command can conduct day to day mission capabilities and requirements that support the warfighter both home and abroad. (Additional information for reason for COMSEC support may be provided based on commands different needs.)

2. Our command requests (x amount) of (name of COMSEC gear/equipment) and (x amount) of (short title of Electronic COMSEC Keying Material). The COMSEC equipment and keys will be in support of circuit (name of circuit being supported). In accordance to reference (a) the required COMSEC support will be for (amount of time support will be required: indefinite, 1 year, 2 years, etc.) The goal is to have all COMSEC requirements by (date of estimated COMSEC support needed).

3. Our EKMS parent command account is: (if known).

4. Point of contact for this matter is (Local Element Control Officer/Security Coordinator) at (555-555-5555) or email: (email of Local Element Control Officer).

CO SIGNATURE

Copy to:
(If required)

Enclosure (10)

SF-700 REQUIREMENTS
FOR
STORAGE CONTAINERS

REFERENCE:

EKMS 1(SERIES) CHAPTER 5, PARAGRAPH 520 (b)(1),

STORAGE REQUIREMENTS:

b. **Required Forms for Storage Containers:** Storage containers for COMSEC material require the following forms:

(1) SF-700: Part (1) of a classified container information form (Standard Form 700) for each lock combination must be placed on the inside of each COMSEC storage container. Current DoD policy considers personal addresses and telephone numbers to be PII and requires Part 1 be sealed in an opaque envelope prior to posting inside the container or door, as applicable. Part 1 is not classified; Parts 2 and 2A will be classified based on the classification of the highest content in the container and must reflect the following derivative and downgrading instructions: "Derived from: 32 CFR 2001.80(d)(3)" "Declassify: Upon Change of Combination".

Note for LECO: COMBINATIONS for safes holding COMSEC material, the SF-700 (Part 2/2A) must be labeled as indicated above.

Example: SF700 with label Part 2.

SECURITY CONTAINER INFORMATION INSTRUCTIONS 1. COMPLETE PART 1 AND PART 2A ON THE INSIDE OF FLAP. 2. DETACH PART 1 AND ATTACH TO INSIDE OF CONTAINER. 3. MARK PARTS 1 AND 2A WITH THE HIGHEST CLASSIFICATION (TAGS) IN THE CONTAINER. 4. DETACH PART 2A AND INSERT IN ENVELOPE. 5. SEE PROPERTY ACT STATEMENT ON REVERSE. 6. IMMEDIATELY NOTIFY ONE OF THE FOLLOWING AGENCIES IF THE COMBINATION IS FOUND OPEN AND UNAUTHORIZED. EMPLOYEE NAME: _____ HOME ADDRESS: _____ HOME PHONE: _____ "Derived from: 32 CFR 2001.80(d)(3)" "Declassify Upon Change of Combination". 1. ATTACH TO INSIDE OF CONTAINER	1. AREA ON POINT (If required) 2. ACTIVITY (If required) 3. DATE & TIME (CONTAINER) 4. DATE AND SIGNATURE OF PERSON MAKING CHANGE	1. DATES (If required) 2. CONTAINER NO. 3. DATE COMBINATION CHANGED	1 1	WARNING THIS COMBINATION IS NOT TO BE REPRODUCED OR DISCLOSED TO ANY OTHER PERSON UNLESS AUTHORIZED BY THE ISSUING OFFICE. IT IS TO BE KEPT IN A SECURE PLACE AND NOT TO BE LOANED OR GIVEN TO ANY OTHER PERSON. COMBINATION Turn to the right until you hear a click. Turn to the right until you hear a click. Turn to the right until you hear a click. Turn to the right until you hear a click. WARNING THIS COPY CONTAINS CLASSIFIED INFORMATION ON WHICH COMBINATION IS BASED. DECLASSIFY UPON CHANGE OF COMBINATION. 3A INSERT IN ENVELOPE.
---	--	---	--------	--

STANDARD FORM 700 (1-81)
Prescribed by GSA/1010-2
20 CFR 2001