(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.

USE THE GREY SECTION WHEN INITIAL LOADING OF EQUIPMENT.

USE THE YELLOW SECTION WHEN DESTROYING KEY FROM EQUIPMENT

Enclosure (5)

MODERN KEY TRACKER											Y / N
Equipment & Serial No.	Partition Code	Universal	Reg. No.	Expiration Date	Date Loaded	Initials	Witness Initials	Date Destroyed	Initials	Witness Initials	Requested new key

USE this side AFTER LOADING key and ZERO. FM SKL

UNIT: _____ (CA 169078)

USE this side AFTER DELETING key from EQP

DATE:

SIGNATURE: _____

PRINT NAME: _____

SIGNATURE: _____

PRINT NAME: _____

Derived from: EKMS 1 (series) -
Declassify on: 28 September 2028

DATE:

SIGNATURE: _____

PRINT NAME: _____

SIGNATURE: _____

PRINT NAME: _____

CONFIDENTIAL WHEN FILLED IN

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)

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)

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.

(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.

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.

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.

(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

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)

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.