NAVAL COMMUNICATIONS SECURITY MATERIAL SYSTEM
1560 Colorado Ave
Andrews AFB, MD 20762

ELECTRONIC KEY MANAGEMENT SYSTEM (EKMS) FOR COMMANDING OFFICER’S HANDBOOK

06 July 2010

DEPARTMENT OF THE NAVY
NAVAL COMMUNICATIONS SECURITY MATERIAL SYSTEM
1560 COLORADO AVENUE
ANDREWS AFB, MD 20762-6108

2250
Ser N5
06 Jul 10

From: Commanding Officer, Naval Communications Security Material System

Subj: EKMS FOR COMMANDING OFFICER'S HANDBOOK LETTER OF PROMULGATION

1. PURPOSE. The information contained in this handbook is provided as a tool for assisting COs, OICs, and SCMSROs in the management oversight of their respective EKMS account.

2. BACKGROUND. Experience has shown that where there is command involvement in the operation and administration of an EKMS account, the end result is efficiency in cryptographic operations and fewer COMSEC incidents and insecurities.

3. INTRODUCTION.

a. This handbook has been prepared in an effort to provide the Commanding Officer (CO), perspective CO (PCO), Officer-in-Charge (OIC) and Staff CMS Responsibility Officer (SCMSRO) with an understanding of COMSEC account and EKMS system requirements and responsibilities. This handbook highlights only those "minimum" requirements set forth by EKMS-1 (series). Analysis has shown that when the CO is knowledgeable of and actively involved in the management of his/her account, that account is more efficiently administered. A copy of this handbook and additional information geared towards CO’s, OIC’s and SCMSRO’s can be found on the NCMS Share Point Portal.

b. This handbook is not intended for use by the EKMS Manager to manage the account as it does not provide in-depth detail of EKMS policy and procedures for account management. For monthly spot checks, the Manager may use individual tabs contained herein.

c. It is recommended that this handbook be included in the command turnover file/folder and maintained in the CO's, OIC or

Subj: EKMS FOR COMMANDING OFFICER'S HANDBOOK LETTER OF PROMULGATION

SCMSRO's personal library of reference material.

d. Throughout this handbook the term “Commanding Officer” or “CO” applies to OICs and SCMSROs as well unless otherwise indicated. The term "EKMS account" applies to COMSEC account.

4. APPLICABILITY. This handbook applies to COs, OICs, and SCMSROs for COMSEC accounts of the U.S. Navy, Marine Corps, Coast Guard and Military Sealift Command.

5. SCOPE. The information contained in this Handbook is derived from policy set forth in national and Department of the Navy COMSEC doctrinal manuals. The guidance herein supplements but in no way alters or amends the provisions of U.S. Navy regulations, SECNAV M-5510.30 (series), and SECNAV M-5510.36 (series).

6. ACTION. Amendment 6 to the EKMS for CO’s handbook is effective upon receipt and incorporates amendments 1 through 5 which were previously promulgated.

7. REPRODUCTION. This handbook is authorized for reproduction and use in any operational environment.

8. COMMENTS. Submit comments, recommendations, and suggestions for changes to the Commanding Officer, Naval Communications Security Material System (NCMS//N5).

/s/

M. C. KESTER

LIST OF EFFECTIVE PAGES

PAGES	**PAGE NUMBERS**	**EFFECTIVE**
FRONT COVER	(UNNUMBERED)	ORIGINAL
LETTER OF PROMULGATION	01 THRU 02	ORIGINAL
LIST OF EFFECTIVE PAGES	i	AMD 6
RECORD OF AMENDMENTS	ii	ORIGINAL
RECORD OF PAGE CHECKS	iii	ORIGINAL
TABLE OF CONTENTS	iv THRU vi	AMD 6
SECTION I	1 THRU 7	AMD 6
SECTION II	1 THRU 11	AMD 6
SECTION III	1 THRU 10	AMD 6
SECTION IV	1	AMD 6
SECTION V	1 THRU 5	AMD 6
SECTION VI	1 THRU 9	AMD 6
SECTION VII	1 THRU 3	AMD 6
TAB A	A1 THRU A5	AMD 6
TAB B	B1 THRU B3	AMD 6
TAB C	C1 THRU C4	AMD 6
TAB D	D1 THRU D5	AMD 6
TAB E	E1 THRU E4	AMD 6
TAB F	F1 THRU F5	AMD 6
TAB G	G1 THRU G3	AMD 6
TAB H	H1 THRU H2	AMD 6
TAB I	I1 THRU I5	AMD 6
TAB J	J1 THRU J2	AMD 6
TAB K	K1 THRU K3	AMD 6
TAB L	L1 THRU L2	AMD 6
TAB M	M1 THRU M2	AMD 6
TAB N	N1 THRU N5	AMD 6
TAB O	O1 THRU O2	AMD 6
TAB P	P1 THRU P3	AMD 6
TAB Q	Q1 THRU Q3	AMD 6
TAB R	R1 THRU R3	AMD 6
TAB S	S1 THRU S3	AMD 6

RECORD OF AMENDMENTS

Identification of Amendment	Date Entered (YYMMDD)	By Whom Entered (Signature, Rank or Rate, Command Title)
AMD 1 (ALCOM 161/10)	2010/10/29	M. DIXSON, IA-03, NCMS
AMD 2 (ALCOM 020/11)	2011/01/29	M. DIXSON, IA-03, NCMS
AMD 3 (ALCOM 085/11)	2011/04/30	M. DIXSON, IA-03, NCMS
AMD 4 (ALCOM 213/11)	2011/12/29	M. DIXSON, IA-03, NCMS
AMD 5 (ALCOM 111/12)	2012/06/29	M. J. PHILLIPS, GG-13, NCMS
AMD 6 (ALCOM 079/13)	2013/04/23	M. J. PHILLIPS, GG-13, NCMS

RECORD OF PAGE CHECKS

DATE CHECKED	CHECKED BY SIGNATURE, RANK/RATE, COMMAND TITLE)	DATE CHECKED	CHECKED BY (SIGNATURE, RANK/RATE, COMMAND TITLE)

COMMANDING OFFICER'S EKMS HANDBOOK TABLE OF CONTENTS

SECTION I

1. GENERAL ADMINISTRATION

a. **GENERAL**. Ultimate responsibility for proper account management and the proper safeguarding, accounting for, handling and disposition of COMSEC material as well as compliance with Navy policy rests with the CO of the account. A flag or general officer in command status, or any officer occupying the billet of a flag or general officer with command status, may either assume personal responsibility for routine COMSEC matters or may designate the responsibility to a senior staff officer (O-4 (or selectee/GS-12/Pay band 2 or above) as a Staff CMS Responsible Officer(SCMSRO). Assignment as SCMSRO must be in writing. This responsibility cannot be further delegated. Commanders below flag or general rank not occupying the billet of a flag or general officer may not delegate a SCMSRO. Exceptions to this policy are identified below:

b. Navy Selective Reserve (SELRES). A Navy SELRES CO may designate an active duty officer in charge (OIC) to sign routine EKMS reports in his/her absence as "acting.” This designation must be in writing and the CO at the first opportunity must chop all reports signed in the CO’s absence. The CO's signature requirement for destruction reports is waived for all Naval Reserve Force EKMS accounts.

c. Marine Corps Reserve. Marine Corps reserve units supported by an Inspector and Instructor (I&I) may assign the supporting I&I as the SCMSRO for routine CMS matters.

2. **EKMS ORGANIZATION**

a. COMSEC Material Control System (CMCS). The protection of vital and sensitive information moving over government communications systems is crucial to the effective conduct of the government and specifically to the planning and execution of military operations. To this end, a system has been established to distribute, control, and safeguard COMSEC material. This system, which consists of production facilities, COMSEC Central Office of Record (COR), distribution and storage facilities (i.e., CMIO), and EKMS accounts, is known collectively as the CMCS.

b. National Security Agency (NSA). The National Security Agency serves as TIER 0 and is the executive agent for developing and implementing national level policy affecting the control of COMSEC material. NSA is also responsible for the production and distribution of most COMSEC material used to secure communications as well as for the development and production of cryptographic equipment.

c. Electronic Key Management System (EKMS) Central Facility (CF). The EKMS CF functions primarily as a high volume key generation and distribution center. As such, it provides commands with keys currently produced by NSA that cannot be generated locally. The CF will interoperate with commands through a variety of media, communication devices, and networks, allowing for the automated ordering of COMSEC key and other materials generated and distributed by NSA.

d. Department of the Navy (DON). The DON administers its own CMCS, which includes Navy, Marine Corps, Coast Guard, and Military Sealift Command (MSC) EKMS Accounts. The DON system implements national policy, publishes procedures, and provides a Service Authority (SERVAUTH) to oversee the management of its complete inventory of COMSEC material.

e. Chief of Naval Operations (CNO). CNO has overall responsibility and authority for implementing National COMSEC policy within the Department of the Navy (DON) and is the resource sponsor for the DON COMSEC program.

f. Commandant of the Marine Corps (CMC). The Command, Control, Communications, and Computers (C4) Department serves as COMSEC resource sponsor for the Marine Corps. The C4 Department coordinates with CNO, COMNAVCYBERFOR, and NCMS to establish, promulgate, and oversee EKMS account management matters unique to the Marine Corps. The C4/CY section is the focal point for requirements and administration for all Marine Corps EKMS accounts.

g. Commander, U.S. Coast Guard C4IT Service Center, Information Assurance Branch (C4ITSC-BOD-IAB): Acts as the USCG Service Authority (SA) and exercises overall authority for USCG COMSEC matters and also serves as the USCG Program Manager and Principal Agent for the USCG COMSEC Program and also functions as the USCG Command Authority (CA). This office promulgates USCG COMSEC Program policy and exercises service wide management of Coast Guard EKMS accounts including hardware and software allowances. The section also acts as principal USCG liaison for COMSEC with CNO, NCMS and the Tier 1’s to ensure that all USCG EKMS Accounts have the necessary resources to operate effectively. The Office coordinates with other Military Services, DIRNSA, other Federal Agencies, State, and Local law enforcement entities to ensure secure/privacy communications interoperability.

h. Commander, Navy Cyber Forces (COMNAVCYBERFOR). COMNAVCYBERFOR implements the DON COMSEC program.

i. Naval Communications Security Material System (NCMS). Under the sponsorship of COMNAVCYBERFOR, NCMS administers the DON EKMS program and acts as the Service Authority (SERVAUTH) for all DON EKMS accounts. For COMSEC purposes, throughout this handbook, the use of "DON" pertains to Coast Guard, Military Sealift Command, Marine Corps and Navy. NCMS serves as the Central Office of Record (COR) and as Tier 1 for Tier 2 accounts.

j. Controlling Authority (CONAUTH). In the context of the COMSEC Material Control System (CMCS), each item of COMSEC material is managed by a designated official known as a Controlling Authority. A "CONAUTH" is responsible for evaluating COMSEC incidents and authorizing the issue/destruction of COMSEC material under their control. By definition, a "CONAUTH" is the command designated as responsible for directing the establishment of a cryptonet/circuit and managing the operational use and control of keying material assigned to that cryptonet/circuit.

k. Immediate Superior in Command (ISIC)/Immediate Unit Commander (IUC). The ISIC/IUC is responsible for the administrative oversight of all COMSEC matters for their subordinate commands. Primarily they validate the operational requirements for EKMS accounts and conduct EKMS account inspections.

l. Commanding Officer (CO)/Staff CMS Responsibility Officer (SCMSRO) / Officer in Charge (OIC). The CO is responsible for the proper operation and administration of the command's EKMS account. Responsibilities applicable to COs apply equally to OICs and SCMSROs unless otherwise indicated.

m. Command Authority (CA/CMDAUTH). The individual responsible for managing Modern Key privileges for the command. Normally the ISIC or Type Commander (TYCOM) is assigned duties as the CA/CMDAUTH for their subordinate units.

n. EKMS Manager. The CO must appoint, in writing, one EKMS Manager and a minimum of one alternate. All alternates must be as familiar with the account as the actual manager, and share equally with the EKMS Manager the responsibility for the proper management and administration of the EKMS account. It is recommended that at least two alternates be appointed. The manager serves as the principle advisor to the CO in all matters regarding COMSEC.

o. STE Material Control (MC) User. There may be an occasion when a STE User will need to routinely draw STE keying material from another User due to their remote location from the command's EKMS Manager. In such situations, the CO may designate, in writing, a STE MC User to assume responsibility for all STE materials on local custody at the remote location.

p. User Representative (UR). The individual(s) assigned within the command that is granted privileges by the Command Authority to order specific Modern Keys for the command.

q. EKMS Clerk. An individual designated in writing by the CO who assists the EKMS Manager and Alternate(s) with routine administrative account matters. Appointment of an EKMS Clerk is not mandatory but is at the discretion of the CO.

r. Local Element (LE)(Using). Local Elements are separate entities, units or commands, internal or external to the parent EKMS account that requires COMSEC material. LEs receive their COMSEC material from the single EKMS account that they are registered to (i.e., their parent account) and never directly from a COR or Tier 0. LEs are normally issued material for use in their assigned equipment. Some LEs are responsible for routinely issuing material to other LEs, and are designated Issuing LEs.

s. Local Element (Issuing). Manage and issue those materials and generate required accounting records. Issuing LE personnel must be appointed in writing and meet the designation requirements outlined in EKMS-1 (series). Issuing LEs must be attached to the command or unit that they will be servicing with COMSEC material.

Note: A Letter of Agreement is required to provide COMSEC support to LE personnel who are part of another command or organization.

t. Witness. Any properly cleared U.S. Government employee/contractor who may be called upon to assist a Manager or LE in performing routine administrative tasks related to the handling of COMSEC material. A witness must be authorized access, in writing, to keying material by the CO.

3. **DUTIES AND RESPONSIBILITIES**

a. **Staff CMS Responsibility Officer (SCMSRO)**

(1) SCMSROs must be designated in writing, by a flag officer and have a security clearance equal to or higher than the highest classification of COMSEC material held by the account. For units without a six-digit account who are LE's of another account but headed by a flag-level officer, a SCMSRO may be appointed.

(2) SCMSROs must sign CMS correspondence and reports as "Staff CMS Responsibility Officer" vice "By direction."

(3) Duties of the SCMSRO cannot be further delegated and must revert to the appointing official in the absence of the assigned SCMSRO.

(4) Specific duties are identical to the COs/OICs duties and responsibilities listed below.

b. **Commanding Officer (CO) / Officer in Charge (OIC)**

(1) COs are **ultimately** responsible for proper management and security of all COMSEC material held by their command and must:

(a) Ensure compliance with established policy and procedures governing the safeguarding and handling of COMSEC material.

(b) Appoint, in writing, qualified and responsible individuals as EKMS Manager and Alternate Manager(s), Local Element (Issuing), and, if desired, an EKMS Clerk.

(c) Appoint, in writing, qualified and responsible STE Material Control (MC) User or Terminal Privilege Authority (TPA) as applicable if the duties are delegated below the EKMS Manager and/or Alternates.

(d) Establish, in writing, a list of personnel authorized access to keying material.

(e) Ensure that training procedures are adequate to meet operational requirements.

(f) Ensure completion and documentation of completion of EKMS Personnel Qualification Standards (PQS) (NAVEDTRA 43462 {series}) by military personnel serving as; EKMS Managers, Alternates, Local Elements (both issuing and using and EKMS Clerks, as applicable.

> **NOTE:** The completion of the above mentioned PQS is not applicable to either MSC, USCG or USMC personnel but can be obtained from: https://www.portal.navy.mil/cyberfor/ncms/default.aspx

(g) Ensure COMSEC incidents are reported within the timeframes set forth in EKMS-1B Article 960 and actions taken to prevent reoccurrence.

(h) Ensure local procedures are established for the timely identification and reporting of any potentially significant changes in life-style, financial status, or any disciplinary problems involving personnel authorized access to COMSEC material.

(i) Conduct unannounced spot checks of the EKMS account at least quarterly in accordance with Article 450 to EKMS-1B (See Section IV).

(j) Receive debriefings from CMS Advice and Assistance (A&A) Training Teams and EKMS Inspectors.

(k) Ensure that comments on personnel performance as Managers/Alternates are included in fitness reports, evaluations, and civilian performance appraisals, as applicable.

(l) Ensure that EKMS Manager assignments are documented in an individual's service record or position description, as applicable.

(m) Ensure an Emergency Action Plan (EAP)/Emergency Destruction Plan (EDP) is established and tested that provides for the protection and/or destruction of COMSEC material during emergency conditions.

(n) Ensure that an inventory of all COMSEC material held is conducted as required by EKMS 1 (series) Chapter 7 on the following occasions:

(1) in conjunction with a Change of Command (COC) or Staff CMS Responsibility Officer

(2) upon change of Change of EKMS Manager (CCIR)

(3) Semi-Annually (Semi-Annual Inventory Report (SAIR))

(4) Account disestablishment

NOTE: Specific types of inventories used, an overview of each and signature requirements can be found in EKMS-1(series) Article 766 and Annex U.

(o) Ensure that assignment of collateral duties to EKMS Managers does not interfere with responsibilities for effectively managing the EKMS account.

SECTION II

1. **EKMS ADMINISTRATION**

a. **Appointment Letter/Memorandum**. An administrative **document, signed by the current CO, formally designating** individuals to duties as an; EKMS Manager, Alternate, Clerk, LE Issuing, LE Using, STE MC User or TPA. The appointment letter/memorandum is maintained locally at the command for a minimum of two years following the relief of an individual. Letters will be updated within 60 days following a change of command.

> **NOTE:** Due to the required retention period of these letters, individuals must be appointed on individual appointment letters. The only exception to this is for LE Users. At the discretion of the CO, consistent with local policy LE Users may be authorized access to COMSEC material through the use of either notes/legend codes for the access list to the space in which they work/are assigned. If an access list is used it must be updated at a minimum of annually or more frequently, as required.

b. **EKMS Library**. Each EKMS account is responsible for maintaining a comprehensive EKMS publications library. The minimum required holdings are outlined in EKMS 1(series) Article 721. The following four publications serve as primary policy documents and should be periodically reviewed by the Commanding Officer. An example of EKMS Library required by EKMS 1(series) is provided in Figure-1.

(1) EKMS-1(series). The "EKMS Policy and Procedures Manual" outlines policy and procedures for receipting, safeguarding, issuing, destroying, inventorying and transferring COMSEC Material.

(2) EKMS-3(series). The "EKMS Inspection Manual "establishes qualification standards for EKMS inspectors and prescribes minimum standards for conducting inspections. It is provided to help the Manager ensure the account is inspection ready at all times.

(3) EKMS-5(series). The "EKMS Cryptographic Equipment Policy Manual" provides policy and procedural guidance to Managers specific to the management of COMSEC hardware.

(4) EKMS 704(series). Local Management Device

(LMD)/Key Processor (KP) Operator Manual.

c. **CMS Form 1**. A locally prepared form that is used to authorize appropriately cleared personnel, one of whom must be the EKMS Manager or Alternate, to receipt for and courier COMSEC material between their command and the CMIO. CMS Form 1 (Figure-2) must be submitted on command letterhead (less messages). Preparation guidance is outlined in EKMS 1(series), Annex H. This form is required only if the command or unit conducts over-the-counter business with CMIO to transfer or receive material. Pickup of COMSEC material from the CMIO is not authorized unless the CMS Form 1 is signed by the current Commanding Officer and updated at a minimum of annually.

d. **USTRANSCOM IMT Form 10**. Defense Courier Service (DCS) is a joint service organization providing courier delivery for qualified categories of classified information to include most COMSEC material. COMSEC material is normally from either the USNDA or shipped to your account by your servicing CMIO, via DCS. Distribution of COMSEC material is normally accomplished using regularly scheduled DCS missions. To receipt for material from DCS, your account must present an up-to-date USTRANSCOM Form 10 **(**Figure-3**)** to the DCS courier(s).

(1) DCS is part the Unified Transportation Command (TRANSCOM) that is sponsored by the United States Air Force. To enter material into the DCS system your EKMS Manager will have to provide DCS with additional TRANSCOM forms that are shipping documents for the material. The TRANSCOM forms are available from the DCS stations and require only the signature of the EKMS Manager or Alternate Manager.

e. **User Representative (UR) Registration Form**. Central Facility (CF Form 1206) must be prepared by the command which reflects personnel authorized to order modern keying material and keying material for STE terminals on behalf of the organization and to interface with the keying system to provide information to key users, ensuring that the correct type of key is ordered. Completed CF Form 1206's are submitted to and approved by the organizations Command Authority (CA). The EKMS Manager may also be designated to serve as UR. It is highly recommended that each alternate is also designated as a UR for the command to enable timely ordering of products during periods of leave, TAD, etc...

f. **Command Handling Instruction**. Each command that holds COMSEC material must generate an instruction delineating how COMSEC material will be handled and stored. Emphasis must be placed on material accountability, Two Person Integrity requirements, security, and the identification of improper practices. This instruction must be provided to all EKMS Managers, Local Elements (issuing/users).

g. **Command Security Procedures**. Local procedures must be established for the identification of any potentially significant changes in life-style, financial status, or disciplinary problems involving personnel authorized access to COMSEC material. Any such changes must be reported to the command Security Manager and if appropriate, the Special Security Officer (SSO).

h. **Emergency Action Plan (EAP)/Emergency Destruction Plan (EDP)**. Every command that holds classified COMSEC or Controlled Cryptographic Item (CCI) material must prepare emergency plans for safeguarding such material in the event of an emergency. For all activities located within the U.S and its territories need consider for natural disasters and acts of terrorism. For commands located outside the U.S. and its territories and deployable commands, planning must include both an Emergency Action Plan (EAP) for natural disasters and an Emergency Destruction Procedures (EDP) for hostile action. Specific requirements and guidance are provided in EKMS 1 (series), Annex M.

i. **Letter of Agreement (LOA).** It is very common for EKMS accounts to have Local Elements who are responsible to a CO other than that of the parent account. In these instances a LOA must be executed between the EKMS account command and the LE's command. LOAs must be updated with every change of command or every three years, whichever occurs first. Annex L to EKMS 1 (series) contains a sample with the minimum required information.

2. **Resource Assistance**: A variety of services and aids are at your disposal to help you prepare for formal inspections, resolve CMS issues, obtain interpretation of COMSEC policy and procedures. These include:

a. **COMFLT/TYCOM/ISIC/CMS A&A Training Team:** When in doubt about a COMSEC matter, encourage your EKMS Manager to contact your CMS COMFLT/TYCOM/ISIC representative or if unavailable, the nearest CMS A&A Training Team. (NOTE: See EKMS-1(series) Chapter 3 for assistance/services provided by CMS A&A Training Team personnel). These are valuable resources and should be used to the maximum extent possible.

b. **NCMS**: If the ISIC or CMS A&A Training Team is unavailable or additional assistance is required, contact NCMS//N7//, the CMS Education and Training Department.

3. **CMS EDUCATION AND TRAINING**. The EKMS Manager MUST develop and implement a CMS training program. The EKMS Manager must conduct training, at a minimum of monthly to ensure that all personnel handling COMSEC material are familiar with and adhere to proper COMSEC procedures. Training for operation of fill device applications and interfaces to end-use items is the responsibility of the program manager of record. Information on how to get training on fill device applications is available through the SPAWAR EKMS Help Desk. Document training locally in accordance with command directives and retain in accordance with EKMS-1(series) Annex T. EKMS Managers are also responsible for the proper training of remote LEs and for ensuring that the Commanding Officers/OICs of their remote LEs (Issuing) are conducting quarterly spot checks as required (EKMS-1(series) Article 465 pertains). EKMS Managers are encouraged to require their remote LE Commanding Officers/OICs to report spot check results; such a requirement should be spelled out in the LOA/MOU between the servicing or parent account and the command being serviced.

a. **EKMS Manager Course of Instruction (COI)**. The Course of Instruction Number (CIN) V-4C-0013 provides personnel the basic skills necessary to fill an EKMS Manager/Alternate position. The COI is a three week course emphasizing EKMS accounting and reporting requirements utilizing the Local Management Device (LMD)/Key Processor (KP), Simple Key Loader (SKL), and Data Transfer Device (DTD). Completion of this course is mandatory for all EKMS Managers and Alternates accounts; **this requirement cannot be waived**.

(1) **Navy/Coast Guard Accounts:** Personnel selected to be an EKMS Manager or Primary Alternate must successfully complete the Navy EKMS Manager's Course of Instruction (COI) (V-4C-0013) **prior to** appointment.

(2) When training cannot be completed prior to appointment due to quota non-availability, operational requirements, etc… personnel appointed must complete the EKMS Manager Job Qualification Requirement (JQR) which is available at https://www.portal.navy.mil/cyberfor/ncms/default.aspx or through the local CMS A&A Training Team.

(3) EKMS Managers completing the above mentioned JQR pending the completion of formal training must complete the Navy

EKMS COI within 90 days of appointment. Alternate EKMS Managers must complete the course within 180 days of initial appointment.

(4) EKMS Managers or Alternates unable to attend formal training within the 90 or 180 day time frame specified above **require** a waiver from NCMS to continue performing duties as the EKMS Manager or Alternate, as applicable beyond the periods specified.

(5) **USMC Accounts:** Personnel selected to be the EKMS Manager or Primary Alternate EKMS Manager must successfully complete the EKMS Manager's Course of Instruction (COI) (V-4C-0013) within 180 days of appointment. Pending completion of formal training, personnel may be appointed as Tertiary Alternates and receive On-The-Job-Training and perform required duties under instruction.

NOTE: Fully qualified personnel who have performed COMSEC duties within the past 12 months may be re-appointed provided that none of the EKMS Manger designation requirements were previously waived.

(6) All military personnel **except** those assigned to MSC, USCG, and USMC accounts appointed or designated as; EKMS Managers, Alternates, Clerks, LE's Issuing and LE Users, appointed/designated, must complete the applicable portions of the latest version of NAVEDTRA 43462 (EKMS PQS) for the position they are fulfilling. The PQS is available from https://www.netc.navy.mil/development.aspx or https://www.portal.navy.mil/cyberfor/ncms/default.aspx under the COMSEC Library tab located on the EKMS Managers page.

NOTE: PQS is not intended to replace formal classroom training. PQS is intended to supplement, through hands-on training at the unit level the skills required by EKMS Managers and Alternate EKMS Managers. While not mandated in EKMS-1 (series), the applicability of PQS or other local training avenues for civilian employees whose position requires access to COMSEC material will be as promulgated in command, ISIC, or TYCOM training or COMSEC policies and should be clarified in position descriptions or individual performance plans.

4. **COMSEC SERVICES**

a. **COMSEC MATERIAL ISSUING OFFICE (CMIO).** Located in Norfolk, VA, CMIO receives, stores, and ships Ready for Issue

(RFI) equipment. CMIO is also the Physical Material Handling Segment (PMHS) for Navy in the EKMS. Commands desiring over-the-counter service from CMIO must have an up-to-date CMS Form 1 on file at the CMIO.

b. **DEFENSE COURIER SERVICE (DCS).** DCS is a joint service organization providing courier delivery for qualified categories of classified information to include most COMSEC material. **DCS should not be confused with NCMS**; they are separate entities and are not related service organizations. Most EKMS accounts receive their COMSEC material via DCS, therefore mobile units, exercise planners, and major staff commands requesting special issues and/or allowance changes must allow sufficient time in their notification to NCMS and CMIO to allow maximum use of regularly scheduled DCS missions. To receipt for material from the DCS, the account must provide an up-to date USTRANSCOM Form 10 to the DCS. An original USTRANSCOM Form 10 with the CO's signature is maintained by DCS. With each delivery/pick-up from DCS, the EKMS account courier must present an identical copy of the USTRANSCOM Form 10 with original signature to the DCS courier.

c. **CMS ADVICE AND ASSISTANCE (A&A) TEAMS.** The CMS Advice and Assistance Program are chartered under the CNO's COMSEC Resources Program. CMS A&A Teams provide front line training to CO's, SCMSRO’s, EKMS Managers and LEs. All EKMS accounts are required to receive a periodic CMS A&A Training Visit no later than 90 days prior to the next scheduled formal inspection. It is **highly recommended** and in the command’s best interest to use the training and assistance provided by the team prior to deployments and when Manager(s) change. The CMS A&A Team should be viewed as an EKMS Manager's personal asset. Their expertise provides a readily available source of technical guidance in all areas related to COMSEC material management. Their charter **"to train and assist"** should be used advantageously at every opportunity by every command handling COMSEC material.

(1) CMS A&A Teams are located at major fleet concentrated areas. The location and geographic areas of responsibilities for each team are identified in **(Figure-5)**. Commands not located in the immediate area of an A&A team will receive their required visits on regularly scheduled trips conducted by the team throughout their area of responsibility. The fixed cycle training visits are funded by the A&A team. Commands which require an "out of cycle” training visit are responsible for funding such visits. These teams are well versed in COMSEC management, policy interpretation, proper COMSEC

handling procedures and can provide training and assistance in the installation, use and restoration of EKMS systems and various (legacy and modern) storage devices.

(2) CMS A&A Teams are not, however, chartered to conduct pre-inspections. At the conclusion of each A&A training visit, the A&A Team Leader will conduct an out-briefing with the CO. This briefing will inform the command of the specific training conducted, areas of weakness and corrective training, personnel who attended, training objectives met as well as any COMSEC Incidents or PDSs which may have been discovered during the visit. All conditions and recommendations discussed during an A&A Training Visit are privileged communications and will not be divulged outside of the command visited.

NOTE: Effective 01 Jan 2013, NLT 30 days following a CMS A&A Training Team visit and every 30 days thereafter, as applicable, EKMS Managers will submit a written status update on any discrepancies documented during the visit to the CO/OIC of the account. Whether communicated via email, memorandum, etc… a copy of the status report(s) will be maintained in the accounts correspondence file with the associated CMS A&A visit report. Do not submit status updates to the servicing CMS A&A Training Team or NCMS.

d. **EKMS Inspections**. NCMS//N7// manages the DON EKMS Inspection Program. All EKMS accounts must undergo a formal EKMS inspection **every 24 months**. This inspection will be unannounced and conducted in accordance with the procedures contained in EKMS 3(series). ISICs are responsible for conducting inspections of their subordinate units. Inspectors must be trained and certified by NCMS//N7//. Inspection results will be forwarded to NCMS//N7// semi-annually.

e. **EKMS TOWN HALLS**: EKMS Town Halls are hosted annually by NCMS and are primarily intended for COs, EKMS Inspectors, and EKMS Managers. Town Halls afford NCMS the opportunity to discuss policy and procedure matters, recurring problems in account management and recommended corrective actions, insecurities and other topics of concern presented by attendees. While attendance at EKMS Town Halls is mandatory for Commanding Officers and EKMS Managers, it is highly recommended that SCMSRO’s and the Primary Alternates attend as well, when possible.

f. **COMSEC Incident Trend Analysis Messages**. Periodically, NCMS publishes COMSEC Trend Analysis messages that provide information on the types of incidents being reported, the common trends that are found from reviewing the incident reports, and recommendations to prevent recurrence.

5. **SELECTING AN EKMS MANAGER**

a. The selection of personnel to serve as EKMS Manager and Alternate(s) should be made carefully. In making your selections, consider the sensitivity and criticality of the communications being protected by the materials you will be entrusting to your EKMS personnel. When personnel are selected through their orders, or for Civilians, their position description (PD), i.e. “Report as Radio Officer/EKMS Manager” a personal interview should be conducted to ascertain the individual’s prior experience and qualifications. Regardless of what the orders state, individuals with no prior experience managing COMSEC material should not be assigned to the EKMS Manager position. They should be assigned to Alternate Manager positions so they have the opportunity to learn under a more experienced individual. Experience, not rank, should be the primary factor when selecting the Manager. Individuals who have achieved significant career milestones are recommended for selection to the Primary EKMS Manager position.

b. An error on the part of a Manager who is assigned too many duties, or who is poorly trained, poorly motivated, or otherwise not suited for the job, can negatively impact mission fulfillment or jeopardize untold amounts of extremely sensitive information.

c. As the EKMS Manager is the principal advisor to the CO in all matters regarding EKMS, it is essential that the CO designate an individual who understands the unit’s mission and COMSEC requirements and displays good common sense and mature judgment. An EKMS Manager should not be chosen solely on accounting or computer skills and should not be assigned on a short term basis because it takes several months to become familiar with the system and to function effectively. Personnel appointed as EKMS Managers, Alternates or Local Element Issuing (LE Issuing) must be permanently assigned to or employed by the command, as applicable dependent upon status (civilian government employee or military member. The use of TAD personnel is not authorized for these positions. An EKMS account must have a designated EKMS Manager and a minimum of one alternate.

d. Designation Requirements for EKMS Manager Personnel. Each numbered account will have an EKMS Manager, and a minimum of one alternate appointed by the current Commanding Officer. For accounts with a Highest Classification Indicator (HCI) of TS, an additional two alternates is **highly** recommended to have at least two personnel who have either the “A” or “B” combinations, as applicable for Two Person Integrity (TPI) purposes during periods of leave, TAD, etc. EKMS Manager personnel must be designated in writing by the current CO, and meet the following requirements:

(1) U.S. Citizen (includes naturalized; resident aliens <u>are not eligible</u>)

(a) For Navy accounts: EKMS Managers must meet the following minimum requirements: Commissioned Officer, E-7 or above (or selectee), GS-7/Pay band 1 or above, all with a minimum of six months government/commissioned service, as applicable which does not include duty under instruction or in training but may include six or more years of prior enlisted service for Commissioned Officers.

(b) For Marine, Coast Guard, and Military Sealift Command Accounts: Commissioned Officer, E-6 (or selectee), GS-7/Pay band 1, or above, all with a minimum of six months government/commissioned service, as applicable which does not include duty under instruction or in training but may include six or more years of prior enlisted service for Commissioned Officers.

(c) Contractor personnel are **<u>not</u>** permitted to serve in EKMS Manager or Alternate positions.

(2) <u>Security clearance</u> equal to or higher than the highest classification of COMSEC material to be held by the account. Appointment can be based on an interim security clearance. If the account is validated for/holds keying material intended for use on SCI/SI circuits, both the EKMS Manager and Alternates **must be** SCI eligible and indoctrinated at the time of appointment.

If the eligibility has been established and is reflected in JPAS but the indoctrination cannot be conducted at the time of appointment, the command may request a waiver from NCMS to afford the time for doing so. If granted, the account must ensure the physical destruction at the account level of keying material used to protect SCI/SI information is conducted adhering to strict Two Person Integrity (TPI) procedures with a minimum of one of the two personnel being SCI indoctrinated. **This will not be waived and is required by National policy.**

Temporary access (interim clearance) may be granted by the

Commanding Officers per the guidance outlined in Art 9-4 to SECNAV M5510.30 however; temporary access for SCI may only be authorized by DON CAF.

(3) Personnel requiring access to COMSEC material must be authorized in writing, the use of "By Direction" is **not** authorized for Letters of Appointment or for granting access to COMSEC material.

(4) EKMS COI (V-4C-0013) Personnel selected to be Primary EKMS Managers must successfully complete the Navy EKMS Manager's Course of Instruction. If possible, personnel selected to be Alternates must also meet this requirement at time of appointment. If this is not possible, persons selected to serve as Alternate Manager(s) must complete the following requirements AND must complete the Navy EKMS COI within six months of their appointment.

(a) CMS Local Element Interactive Courseware (ICW) (A-4C-0031).

(b) EKMS Manager Job Qualification Requirement (JQR), which is available on the NCMS website: https://www.portal.navy.mil/cyberfor/ncms/default.aspx and/or from your local CMS A&A Team.

NOTE: Fully qualified personnel who have performed COMSEC duties within the past 12 months may be re-appointed provided that none of the EKMS Manager Designation requirements were previously waived.

(5) Time Limit. There is no restriction on the time an individual may perform EKMS Manager duties.

(a) Waivers. Commanding Officers are authorized to waive the length of government service required for EKMS Managers. Waivers of this requirement must be documented locally and retained by the account and it's ISIC until no longer in effect. Other waivers must be submitted in accordance with EKMS-1(series) Article 420.

NOTE: Do not submit copies of length of service waivers to NCMS.

(6) Alternate Manager(s). Appointment of a minimum of one Alternate Manager to an EKMS account is required. The number of Alternate Managers beyond one is left to the discretion of the

Commanding Officer. Alternate EKMS Managers must meet the following minimum grade requirements: Enlisted E-6, GS-6/Pay Band 1, or a Commissioned Officer. Alternate EKMS Managers assigned to USCG/USMC in the grade of E5 or higher may be appointed at the discretion of the CO, without the need for a waiver from NCMS.

(7) Temporary Assumption of Manager Duties:

(a) During the temporary absence of the EKMS Manager, the Alternate Manager must administer the account. However, the Alternate Manager may not administer the account for more than 60 days. If the EKMS Manager is absent for more than 60 days, a new EKMS Manager must be appointed.

(b) The Commanding Officer of the account command may authorize an account inventory before, during, or after the temporary absence of the EKMS Manager.

(8) For civilian government employees to be appointed as EKMS Managers or Alternates, the position description must specify EKMS Manager duties as a full-time position, prior to appointment as EKMS Manager.

(9) Position Description for civilian government: employee designated as Primary EKMS Manager must specify the duties as full-time.

SECTION III

1. **COMSEC Incident Reporting**:

a. The COMSEC system has been designed to provide a means for taking corrective action when deviation from established policy and procedures has occurred.

b. These deviations may jeopardize or have the potential to jeopardize national security. However, unless those who handle and manage COMSEC material report deviations specifically identified as COMSEC incidents in a timely manner, corrective actions cannot be implemented. Consequently, all personnel who handle COMSEC play a vital role in this process.

2. **COMSEC Incidents.** Any uninvestigated or unevaluated occurrence that has the potential to jeopardize the security of COMSEC material or the secure transmission of classified or sensitive government information. See EKMS 1 (series) Chapter 9.

a. COMSEC Insecurity - A COMSEC Incident that has been investigated, evaluated, and determined to have jeopardized the security of COMSEC material or the secure transmission of classified or sensitive government information.

b. Reports of any incident must be made irrespective of the judgment of the EKMS Manager or his/her supervisor as to whether or not an incident or possible incident occurred. Disciplinary action should not be taken against individuals for reporting a COMSEC incident unless the incident occurred as the result of willful or gross neglect by those individuals.

3. **Categories and Examples of COMSEC Incidents:**

a. **General**: The incident listing herein is not all inclusive. Additional reportable incidents that may be unique to a given cryptosystem, or to an application of a cryptosystem, will be listed in the operating instructions and maintenance manuals for that cryptosystem. Accordingly, each command must ensure that these documents are reviewed during COMSEC incident/insecurity familiarization training, respectively.

b. COMSEC incidents are divided into **three categories**:

(1) Cryptographic

(2) Personnel

(3) Physical

c. **Examples of Cryptographic Incidents**:

(1) Use of COMSEC keying material that is compromised, superseded, defective, previously used (and not authorized for reuse), or incorrect application of keying material; such as:

(a) Use of keying material that was produced without the authorization of NSA (e.g., homemade maintenance, DES key, or codes).

NOTE: NSA authorization to generate key in the field is implicitly stated in the security doctrine or operating instructions for devices which possess such capability.

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

(c) Unauthorized extension of a crypto period.

(d) Use or attempted use of a Key Generator/Key processor (e.g., KG-83, KGX-93, or KP) beyond its mandatory recertification date without prior approval.

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

(a) A connection between the LMD and a TOP SECRET system/device other than the KP.

(b) Plain text transmission resulting from a COMSEC equipment failure or malfunction.

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

(d) 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 NSA.

(4) Discussion via non-secure telecommunications of the

details of a COMSEC equipment failure or malfunction.

(5) Detection of malicious codes (VIRUSES) on the EKMS system (LMD/KP).

(6) Operational use of an In-Line Network Encryptor (INE) which is not compliant with a mandatory software upgrade by the compliance date without a waiver from NCF or DIRNSA.

(7) Use of a Key Encryption Key (KEK) classified lower than the Traffic Encryption Key (TEK) passed during OTAD/OTAT operations, except during a COMSEC emergency.

(8) Failure to perform KP changeover every three months as described in EKMS-1 (series) Article 238, or more frequently as required. Incident reports submitted to report failure to perform a KP changeover will reflect NAVREINIT2 as the Short Title in Para (2) of the COMSEC Incident report. There is no edition for these items.

(9) Unauthorized extension of Storage Key Encryption Key (SKEK) or Local Key Encryption Key/Host Data Protection Key (LKEK/HDPK) crypto period for the DTD or SKL respectively, as applicable.

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

d. **Examples of Personnel Incidents**:

(1) Known or suspected defection and/or espionage.

(2) Capture by an enemy of persons who have detailed knowledge of cryptographic logic or access to keying material.

(3) Unauthorized disclosure of Personal Identification Numbers (PINs) and/or passwords used on systems, which allow access to COMSEC material/information.

(4) Attempts by unauthorized persons to effect disclosure of information concerning COMSEC material or unauthorized disclosure of information related to COMSEC material.

NOTE: For COMSEC purposes, a personnel incident does not include instances of indebtedness, spouse abuse, child abuse, substance abuse, or unauthorized absence when there is no material missing or no reason to suspect espionage or defection.

e. **Examples of Physical Incidents**:

(1) The physical loss of COMSEC material. Includes whole editions as well as a classified portion thereof (e.g., a classified page from a maintenance manual, keytape segment).

NOTE: If a record of destruction, transfer or relief from accountability report is required but is not available, the material must be considered lost.

(2) The loss or compromise of any of the following:

(a) KP CIKS and non-zeroized KP KSDs-64As (e.g., REINIT 1 AND NAVREINIT 2).

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

(c) Removable media (e.g., floppy disks) containing key or other EKMS information.

(d) KP PINS.

(e) CIK or Card. When the CIK/Card can be identified with a particular secure voice or data terminal and it was not zeroized from the terminal.

(3) Failure to adequately protect or erase a CIK or card that is associated with a lost secure voice or data terminal.

(4) 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 a LE since the previous audit trail review was conducted**, per the requirements outlined in the specific cryptosystem doctrine.

(5) Unauthorized access to COMSEC material by persons inappropriately cleared. **This includes non-establishment of SCI eligibility in JPAS and SCI indoctrination for EKMS Managers, Alternates and LE Issuing when validated for and/or holding such material.**

(6) COMSEC material discovered outside of required accountability or physical control, for example:

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

(b) Material left unsecured and unattended where unauthorized persons could have had access (e.g., leaving a LMD/KP terminal unattended after an Administrator or Operator has logged on and the KP PIN has been entered).

(c) Missing or non-use of required LCI documentation for material issued to user personnel. This includes instances where documents not meeting the criteria of Article 712 are substituted for LCI documents.

(7) Failure to maintain required TPI for TOP SECRET keying material, except as indicated in Article 510.f or where a waiver has been granted. For example:

(a) Single person access to unencrypted TOP SECRET keying material marked or designated CRYPTO, except when authorized in an emergency, (including FDs containing unencrypted TOP SECRET keying material).

(b) Single person access to the KP during TPI mode operations (i.e., generating unencrypted TOP SECRET keying material).

(8) COMSEC material improperly packaged or shipped.

(9) Receipt of classified equipment, and keying material marked or designated CRYPTO with a damaged inner wrapper.

(10) Destruction of COMSEC material by other than authorized means.

(11) COMSEC material not completely destroyed and left unattended.

(12) Actual or attempted unauthorized maintenance including maintenance by unqualified personnel or the use of a maintenance procedure that deviates from established standards.

(13) Tampering with, or penetration of, a cryptosystem; for example:

(a) COMSEC material received in protective packaging (e.g., key tape canisters) which shows evidence of tampering.

(b) Unexplained (undocumented) removal of keying material from its protective technology.

(c) Known or suspected tampering with **or** unauthorized modification of COMSEC equipment.

(d) Discovery of a 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 (e.g., KP) when other indications of unauthorized access or penetration are present.

(14) Unauthorized copying, reproduction, or photographing of COMSEC material.

(15) Deliberate falsification of COMSEC records.

(16) Failure to conduct, document, submit and retain inventories, as applicable and self-reconcile the accounts inventory within the specified time frames unless an extension is granted by NCMS in writing.

> **NOTE:** This includes the inventory of both ALC 4 and ALC 7 material which is locally accountable to the EKMS account.

(17) Any other incident that may jeopardize the physical security of COMSEC material.

4. **Precedence and time frames for initial incident reporting**.

a. IMMEDIATE message within 24 hours if incident involves:

(1) Effective keying material
(2) Keying material effective within 15 days
(3) Incidents involving espionage, subversion, defection, theft, tampering, clandestine exploitation, sabotage, hostile cognizant agent activity, or unauthorized copying, photographing or reproduction of COMSEC material

b. PRIORITY message within 48 hours if incident involves:

(1) Keying material effective in more than 15 days

(2) Superseded keying material
(3) Reserve on Board (ROB) keying material
(4) Contingency keying material

c. ROUTINE message within 72 hours for any other incident not covered above.

> **NOTE:** Neither a local command inquiry nor investigation in progress by an external agency such as NCIS excuses commands from complying with the incident reporting timeframes set forth in this manual. When it is believed that reporting an incident through normal naval message channels might compromise an investigation in progress, the violating command must contact DIRNSA (I31132) or NCMS (N5) by other secure means to provide information concerning the incident.

d. Report incidents involving codebooks per timeframe stipulated by CONAUTH on codebook cover page.

5. **COMSEC Incident Evaluation** - COMSEC incidents will be evaluated within one of three categories:

a. COMPROMISE: The material was irretrievably lost or available information clearly proves that the material was made available to an unauthorized person.

b. COMPROMISE CANNOT BE RULED OUT: Available information indicates that the material could have been made available to an unauthorized person, but there is no clear proof that it was.

c. NO COMPROMISE: Available information clearly proves that the material was not made available to an unauthorized person.

6. **Practices Dangerous to Security (PDS)**. While PDSs are not reportable at the national level (NSA), if allowed to perpetuate, these practices have the potential to jeopardize the security of COMSEC material. All EKMS accounts must conduct PDS familiarization training that will, at a minimum, include a review and discussion of EKMS 1(series) Chapter 10 on an annual basis.

a. Reportable PDS - The following PDSs must be reported OUTSIDE the command to the Controlling Authority, NCMS, or CMIO, as applicable:

(1) Premature or out-of-sequence use of keying material before its effective date, as long as the material was not reused.

(2) Inadvertent (i.e., early) destruction of COMSEC material including; premature zeroization of REINIT 1 CIKS, erroneous flagging and confirmation of destruction for material not destroyed or destruction without authorization of the Controlling Authority (CONAUTH), as long as the destruction was properly documented, and ONLY if re-supply is required.

(3) Unauthorized adjustment of preconfigured default password parameters on LMD (e.g. LCMS SCO password lockout and/or reset.

(4) Failure to return a Key Variable Generator (KVG) i.e. KG-83, KGX-93, KP for Re-Certification when it is due. (This is not applicable to KP TESTPACs at training facilities).

NOTE: See EKMS-5(Series) Article 202 and EKMS-1(Series) Article 535.o for exceptions and shipping notification requirements.

b. Non-reportable PDS - These are some examples of PDSs that do not have to be reported outside the command, but must be reported to the CO:

(1) Improperly completed accounting reports (i.e., unauthorized signatures, missing signatures or required accounting information, incomplete short title information).

(2) Physical COMSEC keying material transferred with status markings still intact.

(3) Mailing, faxing or scanning/emailing (via non-secure fax) SF-153‘s, CMS-25‘s or other documents containing status information or other classified information. If passed electronically, a report of spillage is required per SECNAV M5510.36 and IA Pub 5239.26.

(4) COMSEC material not listed on account inventory when documentation exists to indicate that the material is charged to the account, **OR** COMSEC material not listed on local element (LE) issuing or user inventory when documentation exists at the account level to indicate that the material was issued to the **LE issuing or user, as applicable.**

(5) The issue of keying material in hardcopy form marked/designated CRYPTO, without authorization, to a LE more than 30 days before its effective period.

(6) Late destruction, including key in a fill device, of COMSEC material (i.e., destruction not completed within the timeframes in this manual and superseded key received in a Reserve on Board (ROB) shipment from DCS), except where a waiver has been granted.

(7) Removing keying material from its protective packaging prior to issue for use, or removing the protective packaging without authorization, as long as the removal was documented and there was no reason to suspect espionage. (See EKMS-1(series) Article 769.g note 1 for exception where premature extraction is not deemed a PDS.

(8) Receipt of a package with a damaged outer wrapper, but an intact inner wrapper.

(9) 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.

(10) Failure to maintain OTAR/OTAT logs.

(11) KP-specific non-reportable PDSs:

(a) Failure to perform a KP Rekey annually.

(b) Failure to update and properly record LMD (root, sysadmn, opr, etc…) **every 90 days** or KP PINS every 6 months.

(c) Failure to properly maintain KP CIK/PIN log.

(12) Failure to perform required LCMS backups and/or archives in accordance with EKMS-1 (series) Article 718.d and Annex X paragraph 12.s.

(13) The discovery of non-COMSEC accountable material being accounted for in LCMS.

(14) Loss or finding of unclassified material as defined in EKMS-1 (series) Article 1015.

(15) Failure to report either the receipt of COMSEC material or corrupt Bulk Encrypted Transactions (BET's) within 96 hours of receipt or download, as applicable.

(16) Failure to submit and retain on file inventory completion messages or forms, if submitted online. (Not applicable to inventories used solely for Change of Command)

(17) Failure to conduct, document and retain either quarterly self-assessments or required spot checks.

(18) Failure to report via record message LMD/KP failures 07 days or greater in duration.

(19) Loss of User CIKS for INE's or devices which make use of CIKS. The CIK or card association, as applicable must be deleted promptly from the device. If the associated device is lost or was possibly accessible to unauthorized/improperly cleared personnel submit a COMSEC incident report in accordance with Article 945.E to EKMS-1B.

(20) Non-compliance with mandatory software or firmware upgrades for spare devices or products which do not connect to the GIG, i.e. DTD, SKL, TKL will be documented in accordance with Article 1005.A to EKMS-1B.

SECTION IV

1. **CMS SPOT CHECKS**. In several places throughout this and related DON COMSEC policy manuals, the CO is charged with the ultimate responsibility for the proper management and operation of their command's EKMS Account. The role that the CO plays is a critical element in successful account management. Therefore, it is the CO's duty and responsibility to ensure that unannounced spot checks are conducted on the EKMS Account (Vault) and Work Centers where COMSEC material is handled used and stored. Ensuring that unannounced spot checks are conducted has proven to be of significant value. Potential problems can be identified and corrective measures taken prior to an official inspection. The guide for Commanding Officer's Unannounced Spot checks is included in Section VII.

2. The CO may delegate **no more than two** of his four quarterly spot checks to the Executive Officer. SCMSROs may delegate two of the four spot checks to the Communications Officer (COMMO)as long as the COMMO is not designated as the EKMS Manager or Alternate.

3. Additional mandated spot checks:

a. EKMS Managers or Alternates **must** conduct a minimum of one spot check per calendar month on supported Local Elements (LE's). It is recommended that the same LE's are not visited every month to gain a better perspective on the account as a whole and to provide training and oversight throughout the organization and not just to one or two LE's.

> **NOTE:** For LE's where it is not practical for the EKMS Manager or Alternate to conduct spot checks on the LE, they will be conducted by the LE's OIC. The same will hold true, the OIC may delegate **no more than two** of his four quarterly spot checks to a designated individual, with the results submitted to the EKMS Manager or Alternate of the EKMS numbered account.

b. At a minimum of quarterly, the EKMS Manager or an Alternate must conduct a self-assessment of the account using the applicable sections of EKMS-3(series). The same criteria is used during an ISIC inspection therefore, quarterly reviews following the same criteria should result in the account doing well during official inspections.

SECTION V

1. **EKMS INVENTORIES**. EKMS inventories are required to ensure COMSEC Material is continuously and properly accounted for. There are four occasions for the inventories to be conducted:

a. Semi-annually: All COMSEC material (including equipment and publications) assigned AL Code 1, 2, 4, 6, and 7 must be inventoried semi-annually (twice each calendar year (CY)).

b. Change of EKMS Manager: All COMSEC material will be inventoried and the results will be retained at the command in accordance with Annex T.

c. Change of Command (COC), OIC or Staff CMS Responsibility Officer: Prior to the relief or detachment of the Commanding Officer, **all** COMSEC material will be inventoried.

d. Account Disestablishment: Accounts being disestablished must complete and return inventories to the COR as stated Article 810.

2. **Who Can Conduct an Inventory.** Inventories must be conducted by the EKMS Manager (or Alternate) and a properly cleared witness except as discussed in paragraph 3 below. The individuals who perform the inventory should remain together for the entire evolution; i.e. do not swap out witnesses in the middle of the inventory. Change of EKMS Manager Inventories should be performed by the outgoing and incoming EKMS Manager. (This includes LE Issuing Manager) Change of Command inventories should be signed by the outgoing CO/OIC or SCMSRO, as applicable. The incoming CO/OIC or SCMSRO (as applicable) may initial, if desired, but it is **not required**. If an individual is physically incapacitated in the middle of the inventory, the CO will decide if the inventory must be started over or if the replacement will be allowed to pick up where the incapacitated individual left off.

3. **Local Element Material**. At the discretion of the EKMS Manager, consistent with local, ISIC and/or TYCOM policy the EKMS Manager can generate and provide the LE with a list of all the material charged to the LE, and the inventory can be performed by the person having local custody responsibility for the material and a qualified witness. In situations where the LE is co-located with the Primary Account it is recommended that the EKMS Manager and his/her witness conduct the LE inventory. Remotely located LEs should perform the inventory of material charged to

them and return the properly completed inventory to the EKMS Manager.

a. When the inventory is presented for signature there may be line-outs for material that was transferred or destroyed after the report was generated. However, for any material altered or lined out, supporting documentation must exist on file with the Manager and the inventory be annotated with applicable dates and/or transaction numbers.

> **Note**: Line outs or adjustments should be minimal and can be minimized through the EKMS Manager generating the required monthly Change of Account Location (COAL) inventory in accordance with EKMS-1(series) Article 766.b.4.

4. **TIER 1 Semi-Annual Inventory Report (SAIR) Process**.

a. Inventories will be conducted, at a minimum of semi-annually and will include; all keying material, equipment and publications as well as required page checks.

b. Semi-annually based on the units EKMS account number the COR will electronically transmit a ***Request for Inventory Transaction*** to each account. Once opened, this request will prompt the account to submit a SAIR. No later than 30 days after receipt of the initial Request for Inventory Transaction, the account must generate an inventory with the COR as the destination EKMS ID and submit the inventory via the message server to the COR. Procedures for electronically submitting a SAIR can be found in EKMS-704(series).

c. The process above is not related to the physical conduct of an inventory but is used to identify accounting discrepancies between the COR and the units Accountable Item Summary (AIS). Accounts have up to a maximum of 90 days to; generate and submit an electronic inventory to the COR; generate the working copies of inventories for the local account and each local element registered in LCMS; complete the physical inventory, including applicable page checks and report completion by either message or completion of the inventory completion form on the NCMS Web Site, and self-reconcile the inventory.

d. The COR must be notified by either record message or submission of an online inventory completion form (as discussed in Article 766 to EKMS-1 (series) upon completion of the physical inventory.

e. After electronic submission of the SAIR to the COR, the COR will respond with an electronic Inventory Reconciliation Status Transaction (IRST) (Type 17) that will; if no discrepancies are noted, enable the SAIR to be processed in its entirety, automatically update the accounting data, close out the inventory cycle and notify the account of the completed inventory reconciliation.

f. If discrepancies are identified in the IRST, it is the responsibility of the EKMS Manager to work diligently with the COR to resolve any discrepancies in a timely manner. Guidance to assist the manager in the understanding and resolution of inventory discrepancies can be found in EKMS-1 (series) Annex AK. If not resolved and manual intervention is necessary, the COR will correspond with the account to correct the discrepancies. The COR Manager will assist the account in clearing all discrepancies that appear on the IRST. It is the responsibility of the EKMS Account Manager to actively pursue resolution of all IRST discrepancies in order to achieve a final reconciliation of the inventory. The IRST must be reconciled with the COR and all discrepancies resolved or documented to the COR Account Manager within 90 days from the date of the original request for inventory transaction.

g. The COR will monitor the response to inventory transactions and will notify commands that fail to return a reconciled inventory within 30 days.

5. **IRST**. The IRST is an electronic bit for bit comparison of the account data on file at the COR against the data on file at the account. Multiple IRSTs are not necessarily an indication of poor account management. If the account performs many daily transactions multiple IRSTs are likely. To keep the number of IRSTs to a minimum, it is strongly recommended that Account Managers generate a Change of Account Location (COAL) inventory as described below in paragraph 8.

6. **SNAPSHOT**. Regardless of the accounting system in use, CO's should recognize that the inventory is similar to a bank account checkbook. Like a checkbook the inventory represents a snapshot in time and it must be balanced frequently to ensure discrepancies are found in a timely manner. When problems exist, communication with the COR is essential.

7. **COMMON ACCOUNT DATA (CAD)**:

a. The CAD is the primary means used by the COR to determine Point Of Contact Information for EKMS Accounts. Failure to maintain accurate and up-to-date CAD data could result in:

(1) Failure to receive electronic key

(2) Delays in receiving physical keymat or COMSEC equipment as a result of an incorrect shipping address.

(3) Delays in obtaining assistance from NCMS, A/A Teams, the EKMS Technical Support Center or other agencies due to incorrect contact information. e.g. phone numbers, email addresses, etc.

b. EKMS Managers must frequently review and update their CAD, and ensure the following information is correct:

(1) The names of the EKMS Manager and Alternates.

Submarine accounts with Blue and Gold crews only: In the Primary Manager Field: The present manager of the active crew preceded by the first letter of the active crew, i.e., G ITCS Longfellow. In the Alternate Manager Fields: First line will be the Primary Manager of the inactive crew followed by **all** Alternates preceded by the first letter of the crew, i.e., B ENS Jones; G ENS Smith.

(2) Primary and Alternate phone numbers where the EKMS Manager/Alternate can be reached. If Duty Officer numbers are provided, ensure the Duty Officers are provided POC information for the Account Managers.

(3) Mailing Address: Outer wrapper information.

(4) NIPRNET and SIPRNET email addresses for the EKMS Manager and Alternates.

Submarine accounts with Blue and Gold crews only: Enter only the SIPRNET email address for each alternate preceded by the first letter of the crew, i.e., B jonesj(at)ohio.navy.smil.mil; G smithj(at)ohio.navy.smil.mil. If sufficient room is not available to enter the email address for all alternates, then enter only one alternate per crew. If the SIPRNET and NIPRNET email addresses are the same with the exception of ".smil" then enter as: B jonesj at ohio.navy(.smil).mil.

(5) Name, rank/grade and NIPRNET and SIPRNET address

of the Commanding Officer. (This data will be maintained and updated in one of the blank Alternate Manager fields.

Submarine accounts with Blue and Gold crews only: For CO’s: Will reflect only the name/rank preceded by the first letter of the crew, i.e., B CAPT. Johnson; G CAPT. Marks (or use CDR, as applicable in lieu of CAPT).

NOTES: (1) CAD data will be reviewed and updated at a minimum of semi-annually in conjunction with the SAIR inventory, when a Change of EKMS Manager or Change of Command inventory is conducted and when a change in EKMS Manager or Primary Alternate occurs. In doing so, phone numbers, email addresses, etc… should also be verified and updated, as applicable.

(2) USMC Accounts may use either the name of the Commanding Officer or ISIC, as desired in meeting the requirement noted in paragraph above.

8. **CHANGE OF ACCOUNT LOCATION (COAL) INVENTORY**. A primary management tool intended to assist EKMS Managers in determining the health and status of the account. **Except as indicated below,** at a minimum of monthly, EKMS Managers will generate a COAL inventory and wrap/submit the inventory to Tier 1 to obtain an Inventory Reconciliation Status Transaction (IRST) in accordance with the procedures outlined in the EKMS-704C.

a. Submarines at-sea are exempt from the monthly requirement noted above when deployed but will generate a COAL within 30 days prior to departure and upon return from at-sea period.

NOTE: An up-to-date printout of Accountable Items (A/I) Summary. (EKMS accounts and Local Elements). At the account level, either a printed up-to-date Change of Account Location (COAL) inventory or AIS may be maintained as discussed in Article 763.c (note) to EKMS-1(series).

SECTION VI

1. **EXAMPLE SHEET/FIGURE.** The COMSEC examples are provided to assist the CO's in identifying required forms and publications required by the account Manager to manage the EKMS account.

FIGURE-1

EKMS LIBRARY

All accounts must maintain a COMSEC Library which, consists of the below reflected manuals and instructions. Access to the NCMS Share Point Portal requires a valid PKI token and can be found here.

NOTE: EKMS Managers must also ensure supported LE's have access to or are provided copies of all COMSEC manuals and instructions required in the operation of the LE account.

a. LMD/KP Operator's manual, EKMS 704 (series).

b. EKMS Intelligent Computer Aided Trainer (ICAT) (also known as the LCMS CBT). This software is embedded on the LMD platform.

c. EKMS Manager JQR.

d. Local Element Issuing CBT.

e. COMLANTFLT/COMPACFLT/COMUSNAVEURINST C2282.1 (series) – Basic Shipboard Allowance of COMSEC Material. (**Surface ships only**) It can be obtained from COMUSFLTFORCOM at(757) 836-5853 or via SIPRNET at: www.ffc.navy.smil.mil.

f. EKMS-1(series) - EKMS Policy and Procedures Manual for Phase 4 EKMS Tiers 2 and 3.

g. EKMS-3(series) - EKMS Inspection Manual.

h. EKMS-5(series) - Cryptographic Equipment Manual.

i. COMDTINST 5510.23 – Coast Guard Classified Information Management Manual. (**COGARD accounts only**).

j. NAG-53(series) – Keying Standard for Non-Tactical KG-84/KIV-7 Point to Point Circuits (**Shore-based accounts only**)

k. NAG 16(series) – Field Generation and Over-the-air Distribution of tactical Electronic Key. (**Required only if the account is involved in OTAT/OTAR operations**).

l. NSA Mandatory Modification Verification Guide (MMVG)- Is available via the NCMS **SIPR** Portal at: http://www.fleetforces.navy.smil.mil/netwarcom/ncms/ekmsmanagers/default.aspx.

m. OPNAVINST 2221.5(series) - Release of COMSEC Material to U.S. Industrial Firms Under Contract to USN. (**Required only by those accounts which have an occasion to release COMSEC material to contractors**).

n. SECNAV M5510.36(series) - Information Security Program

o. SECNAV M5510.30(series) – DON Personnel Security Program (PSP) Instruction.

p. OPNAVINST 5530.14(series) - Physical Security and Loss Prevention.

q. SECNAVINST 5040.3 (series) - Naval Command Inspection Program. Available at: http://www.dtic.mil/whs/directives/links.html

r. NAVICPINST 2300.4(series) - Utilization and Disposal of Excess COMSEC Material.

s. NAVICPINST 5511.24(series) - Classified Electronic COMSEC Material in the Navy Supply System.

t. OPNAVINST 2221.3(series) COMSEC Equipment and Maintenance Training.

u. CJCSI 3260.01(series) - Joint Policy Governing Positive Control Material Devices. (**Required only if account holds SAS material**). The most recent version is available by calling J3 at the Chairman of the Joint Chiefs of Staff Office, Commercial: 703-692-6932 or DSN 222-6932.

v. SDIP 293 - NATO Cryptographic Instruction. (**Required only if the account holds NATO material**). Available from: www.iad.nsa.smil.mil/resources/library/nato/index.cfm

w. AMSG 600 – NATO Communications Security Information. (**Required only if the account holds NATO material**).

FIGURE-2

CMS FORM 1

____
(DDMMYY)

From: ________________________________
(Command title and mailing address)

To: CMIO Norfolk VA

Subj: AUTHORIZATION TO DROP-OFF AND RECEIPT FOR AND COURIER COMSEC MATERIAL

Ref: (a) EKMS-1(series)

1. Per reference (a), the below named individuals are authorized to drop off or receipt for and courier COMSEC material for the above EKMS numbered COMSEC account command:

RATE/RANK/ NAME (Last, First, MI) DOD ID SECURITY POSITION
SIGNATURE CLEARANCE
GRADE

LAST ENTRY—

2. a. **EKMS ID number: __________**
b. **Highest Classification Indicator (HCI):______**
c. **Command Telephone number(s)**
d. **ISIC: ____________________________**

3. I certify that the individuals identified above are assigned to my command; are authorized to drop off, receive and courier COMSEC material for the above command/account; and possess a security clearance equal to or higher than that of the COMSEC material being handled.

AUTHORIZING OFFICIAL SIGNATURE:

____

RANK/GRADE NAME (Last, first, MI) POSITION (e.g., CO, OIC)

____

(CMS Form 1)

NOTE: By direction signatures are not authorized.

FIGURE-3

USTRANSCOM IMT 10

Part I: All Account Types			
Account Delivery Address (1)	Account Mailing Address and Fax Number (2)	After Duty Hours Contact (3)	Account Expiration Date
		Organization/Group NIPR and SIPR E-Mail NIPR: (4) SIPR:	

Customers must coordinate with their servicing Defense Courier Station if there are any additions and/or deletions concerning the authorizing official or the individuals named below.

Name	Grade/Rank	Telephone Number E-Mail Address	Signature
(5)			

Clearance statement: The authorizing official acknowledges that the individuals listed above are authorized to enter and receive qualified material IAW DOD 5200.33R; and possess an appropriate personal security clearance for the qualified material they will be entering or receiving

Date (6)	Authorizing Official (Name, Grade, Title) (7) E Mail:	Rotation Date (8)	Signature (9)

Part II for Government Contractor Accounts:

THIS CERTIFIES THAT THE INDIVIDUALS IDENTIFIED HEREIN POSSESS A VALID SECURITY CLEARANCE TO THE DEGREE OF THE HIGHEST CLASSIFIED MATERIAL THAT COULD BE RECEIVED AND/OR ENTERED BY THE ACCOUNT.

Date	Government Security verification authority (Name/Grade/Position/Organization) E Mail:	Signature

Part III for Consolidated Control Account (CCA) Authorization:
PERSONNEL LISTED ON THE USTRANSCOM IMT 10 FOR ACCOUNT [*Specify Courier Account Number-Station Run Code-DoDAAC*] ARE AUTHORIZED TO ENTER/RECEIVE MATRIAL ON BEHALF OF THE ACCOUNT (S) LISTED IN PART I.

Date	Authorizing Official (Name, Grade, Title) Email:	Rotation Date	Signature

Part IV Forces Afloat Required Contact Information

Point of Contact	POTS Number (Surface Vessels)	Commercial/DSN	E-Mail Address
Operations Officer			
Executive Officer			
Account Validation (For Courier Station Use Only) Validating Courier (Name and Grade)	Date	Signature	

USTRANSCOM IMT-10 Defense Courier Account Record

1. Account Delivery Address
2. Account Mailing Address and Fax number
3. After Duty Contact telephone number
4. Organization/Group NIPR and SIPR email addresses
5. Authorized individuals
6. Date
7. Authorized Official's Information
8. Rotation Date
9. Signature

FIGURE-4

CMS A&A TRAINING TEAM SERVICES

1. **General:** CMS A&A Training Teams can provide assistance in resolving general or specific problems and in most cases this can be done over the telephone. When required, a date can be arranged for a Training Team to visit a command.

2. **Request for Service(s):** Submit a request for service(s) to the closest CMS A&A Training Team in your area (see Figure-5) for location.

3. **Types of Services:** CMS A&A Training Teams provide the following services:

a. **CMS TRAINING VISITS:**

(1) Training visits provide the basis for self-improvement and are not to be confused with a formal EKMS Inspection. Training visits last six to eight hours, are strictly informal, and provide guidance on the policy and procedures for COMSEC material.

(2) Results of a Training Team visit are not reported outside of the command visited. A debrief to the Commanding Officer (or designated representative) and the Manager is provided covering specific areas of training and the personnel involved.

(3) Training visits encompass the EKMS account and LEs. (NOTE: Training for LEs must be coordinated and scheduled by the parent EKMS account with the CMS A&A Training Team.)

b. **EKMS FOR COMMANDING OFFICERS:**

(1) This mandatory training is for COs, SCMSROs, and OICs to enable them to effectively monitor their account's compliance with established procedures. Training lasts approximately two hours and may be conducted at the account command or other location as coordinated by the requesting command.

c. **EKMS INSPECTOR TRAINING:**

(1) EKMS Inspectors must be retrained every 36 months to maintain their authorization to inspect EKMS accounts.

(2) This training enables ISIC staff representatives to conduct formal EKMS Inspections of subordinate account commands.

(3) EKMS Inspector training is conducted by all CMS A&A Training Teams. EKMS Inspector training consists of 8 hours of classroom training instruction and participation in a minimum of one periodic A&A Training visit and assist in an actual EKMS Inspection.

(4) EKMS Inspectors are appointed by the EKMS Inspectors organization based on a letter of certification recommending assignment from NCMS. NCMS reserves the right to rescind EKMS Inspector recommendations when the management and health of a DoN EKMS account which has been recently inspected is discovered to not be in compliance with DoN policy and such was not identified and documented in the Inspectors official report.

d. **EKMS LOCAL ELEMENT/USER BRIEF AND TRAINING**:

Provides EKMS Managers with supplemental training for their LEs. This training lasts approximately three hours and can be provided at the account command orate the CMS A&A Training Team site.

e. **EKMS MANAGER WORKSHOPS**:

Addresses changes to EKMS policy and procedures, recurring problems in account management, insecurity trends and topics of concern introduced by attendees. EKMS workshops are primarily for COs, EKMS Inspectors, and EKMS Managers.

f. **STE/DTD/SKL BRIEF**:

Provides guidance and training on handling and safeguarding of electronic devices.

g. **LOCAL MANAGEMENT DEVICE/KEY PROCESSOR (LMD/KP) TRAINING (EKMS MANAGEMENT TEAM):**

CMS A&A Training Team personnel can provide training and assistance on the operations and management of the Local Management Device/Key Processor (LMD/KP) or the software used on the LMD which is Local COMSEC Management System (LCMS.)

CMS A&A TRAINING TEAM AREA OF RESPONSIBILITY

CMS A&A Training Team responsibilities are divided among 10 teams, each responsible for a specific geographical region as shown below:

ATLANTIC REGION

CMS AA Washington, DC. Delaware, Maryland, Northern Virginia (including Quantico & Dahlgren), and the District of Columbia.

CMS AA Norfolk, VA. Illinois, Indiana, Iowa, Kansas, Kentucky, Michigan, Minnesota, Missouri, North Carolina (Elizabeth City and Cape Hatteras only), Ohio, Virginia (less Northern Virginia, Dahlgren, and Quantico), West Virginia, and Wisconsin.

CMS AA Mayport, FL. Alabama, Caribbean (Andros Island Test Range), Florida, Georgia, Guantanamo Bay, Lesser Antilles, Louisiana, Mississippi, Panama, Puerto Rico and Texas.

NCMS DET Groton, CT. Connecticut, Iceland, Maine, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont, and Newfoundland.

NCMS DET Camp LeJeune, NC. Arkansas, North Carolina (less Elizabeth City and Cape Hatteras areas), Oklahoma, South Carolina and Tennessee.

PACIFIC REGION

CMS AA PEARL HARBOR, HI. Hawaii, Midway Island, All EASTPAC.

CMS AA PUGET SOUND, WA. Alaska, Idaho, Montana, Nebraska, North Dakota, Oregon, South Dakota, Washington, and Wyoming.

CMS AA SAN DIEGO, CA. Arizona, California, Colorado, New Mexico, Nevada, and Utah.

CMS AA FAR EAST YOKOSUKA FE. Japan, Korea, Singapore, Mariana Islands, Philippines, and all WESTPAC/INDIAN OCEAN between 060E and 165E.

EUROPEAN REGION

CMS AA NAPLES, ITALY. Europe including the Mediterranean Sea, Indian Ocean (West of 060E), Persian Gulf and United Kingdom.

SECTION VII

1. **CO SPOT CHECK GUIDE**. This guide consists of a series of 13 EKMS Manager/Local Element Issuing (as applicable) and 6 EKMS Local Element "Spot Checks". The check-off sheets provide supplemental material for conducting the required unannounced spot checks.

Commanding Officers and Executive Officers are encouraged to conduct COMSEC spot checks by selecting one or several of the 19 enclosed "Check off Sheets" randomly each quarter.

EKMS Managers and/or Alternates must conduct a minimum of one spot check per calendar month (12 total per CY) on supported LE’s. It is highly recommended that other supervisory personnel (LCPO, Division Officers, etc… or their service-specific equivalents) conduct training and spot checks in their work centers as well. Things to consider reviewing:

a. Does the security clearance information held by the Division match that held by the Security Manager and is such reflected in JPAS?

b. Observe two personnel performing destruction of physical or electronic key. Were both individuals performing the destruction in agreement that the material was superseded and authorized for destruction? Did the 1st person read off the short title, edition, and reg/serial number to the 2nd person? Did they reverse the role with the 2nd person reading off the information to the 1st person who was verifying the destruction document?

c. Observe the conduct of a watch to watch inventory. Did the personnel conducting the inventory also use/review the corresponding CMS-25’s (destruction documents) to ensure all segmented material was accounted for or documented as destroyed, as applicable?

d. Review the work centers OTAD/OTAR/OTAT logs, if applicable. For key which has been superseded/destroyed, does the log reflect the signature and/or initials of the personnel zeroizing the key?

e. Did the Manager/Alternate follow proper material receipt procedures?

f. Look around the space for the following;

(1) Is the space outwardly identified as a Restricted Area?

(2) Is a visitors log in place and being properly used/maintained?

(3) Is there a SF-701 (Daily Activity Checklist) posted and is it being used, as required?

(4) Is there a SF-702 (Open/Closure Log) for security containers in use? (two are required for TPI containers). Is it being used properly (opened by/closed by/checked by)

This guide reflects current standards imposed by EKMS-1 (series), EKMS-3 (series), EKMS-5 (series), SECNAV M5510.30 (series), SECNAV M5510.36 (series), OPNAVINST 5530.14(series) and National level policy.

2. **SPOT CHECK SHEET**. Is provided and listed as follows:

a. Spot Check sheets for EKMS Manager/Local Element Issuing (As applicable):

TAB A - EKMS ACCOUNT SECURITY

TAB B - MANAGER PERSONNEL

TAB C - LMD/KP

TAB D - RECORDS AND FILES

TAB E - EKMS ACCOUNT

TAB F - INVENTORIES

TAB G - STORAGE AND SECURITY

TAB H - AMENDMENTS AND MODIFICATIONS

TAB I - ELECTRONIC KEY

TAB J – TRAINING

TAB K - EMERGENCY ACTION PLAN (EAP)

TAB L - LOCAL HANDLING PROCEDURES

TAB M – VAULT CHECK-LIST

b. Spot Check Sheets for Local Element:

TAB N – SECURITY

TAB O - WATCH TO WATCH INVENTORY

TAB P – DESTRUCTION

TAB Q - COMSEC PROCEDURES AND HANDLING

TAB R - ELECTRONIC KEY

TAB S - EMERGENCY ACTION PLAN (EAP)

TAB A

COMSEC SPOT CHECK
EKMS MANAGER/LOCAL ELEMENT ISSUING
(AS APPLICABLE)

SECURITY

DATE: ________

Yes No

1. Is the space/compartment or vault outwardly identified as "RESTRICTED AREA"? [OPNAVINST 5530.14 (series), Article 210.g.4, 218.a.4] [**MCO 5530.14(Series) USMC accounts only**] ___ ___

2. Is visitor identification, security clearance and need to know properly verified? [EKMS 1(series), Article 505.b, 550.e; SECNAV M-5510.30 (series), Article 11-1 paragraphs 2,3] ___ ___

3. Is a visitor register in-use, properly maintained and retained for 1 year from the date of the last entry? [EKMS-1(series) Article 550.e.(1)(d), Annex T] ___ ___

4. Do all personnel having access to COMSEC material have a clearance equal to or greater than the classification of the material? [EKMS-1(series) Article 505.a] ___ ___

NOTE: LMD/KP System Administrator's and Operator's must have a minimum clearance level of SECRET.

5. If the account holds material for SCI/SI circuits, are Account Managers SCI eligible and indoctrinated or has temporary access been granted by DON CAF?{EKMS-1 (Series), Article 412.d;SECNAV M5510.30 Art 9-4.4 ___ ___

6. Are the names of individuals with regular duty assignments in the facility, on a formal access list signed by the current CO/OIC/SCMSRO, and has the list been updated whenever the status of an

individual change or at a minimum of annually?
[EKMS-1(series) Article 505.d (2)] ___ ___

7. Has formal facility approval been
given in writing by the ISIC, IUC or higher
authority to install, maintain, operate and
store classified COMSEC material? ___ ___
[EKMS-1(series) Article 550.d]

NOTE: Marine Accounts are required to have a Physical Security Survey (PSS) conducted biennially by a school trained Military Provost Officer.

8. Are applicable security controls (e.g., guards
and alarms) in place in accordance with SECNAV-M
5510.36, Chapter 10? [EKMS-1(series),
Article 520.a(3)] ___ ___

9. Are combinations changed as required;
when a new lock is put in-service or replaced,
upon transfer or reassignment of personnel
who have access, biennially or when
compromised)? [EKMS-1(series) Article 515.b] ___ ___

10. Is a Security Container Information
Form (SF-700) maintained for each lock
combination and placed **inside** each
COMSEC security container? [EKMS-1(series),
Article 520.b SECNAV-M 5510.36, Article 10-12] ___ ___

11. Are combination records for COMSEC
containers recorded in sealed envelopes, kept
on file in a secure central location
designated by the commanding officer and
available to appropriate duty officers
for emergency use? [EKMS-1(series) Article 515.e] ___ ___

12. Except in an emergency, are combinations
to the COMSEC Account vault/COMSEC Facility/
security containers restricted to the EKMS Manager
and Alternates only? [EKMS-1(series) Article 515.c(1)] ___ ___

13. Are sealed combination records
inspected for signs of tampering and
documented monthly? [EKMS-1(series) Article 515.f (6)] ___ ___

14. Do storage containers for COMSEC

material meet minimum security requirements for the highest classification of material stored therein? [EKMS-1(series), Article 520.c, 520.d, 520.e, 520.f, SECNAV-M 5510.36, Chapter 10] ___ ___

NOTE: Effective 01 July 93 commands are not authorized to externally modify GSA approved security containers or vault doors. If external modifications are made after this date, the containers or vault doors are <u>no</u> longer authorized to store <u>any</u> classified material. [EKMS-1(series), Article 520.f]

15. In a **non-continuously** manned COMSEC facility, is a security check conducted and recorded on a SF-701 at the end of the working day? [EKMS-1(series) Article 550.d (3)(b); SECNAV-M 5510.36, paragraph 7-11] ___ ___

16. If a COMSEC facility is **continuously** manned, is a security check conducted and recorded at least once every 24 hours? [EKMS 1 (series), Article 550.d (3)(a)] ___ ___

17. If a facility is in an area posing a high risk of capture by an adversary and the facility will be unmanned for periods greater than 24 hours (e.g., during weekends and holidays), is the facility protected by an approved IDS? [EKMS-1(series) Article 550.d (3)(c)] ___ ___

18. Are completed SF-701's retained on file for 30 days beyond the last date recorded? [EKMS-1(series) Annex T] ___ ___

19. Is a Security Container open/closure log (SF-702) maintained for each lock combination of a COMSEC storage container? [SECNAV-M 5510.36 7-11; EKMS-1(series) Article 520.b (2)] ___ ___

NOTE: A separate (SF-702) must be used for each combination set on an X-07, X-08 or X-09 lock.

20. Are completed SF-702's retained for 30 days

beyond the last entry recorded on the form? [EKMS-1(series) Annex T; SECNAV M5510.36 Article 7-11]] ___ ___

21. Are SF-700's protected in individually wrapped in aluminum foil and protectively packaged in an SF-700 envelope? [EKMS-1(series) Article 515.f] ___ ___

a. Are SF-700's sealed using transparent lamination or plastic tape? ___ ___

b. Names, addresses and phone numbers of individuals authorized access to the combination clearly recorded on the front of the envelope? ___ ___

NOTE: The use of see recall roster is not authorized.

c. Proper classification markings and downgrading instructions on Part 2 and 2A? ___ ___

NOTE: On Part 2, the carbon writings tend to fade. It is recommended that black/blue or black ink be used to write in the information on both Parts 1 and Part 2.

22. Are classified material storage containers free of external markings that indicate the classification level of material stowed in the container? [SECNAV M5510.36 Article 10-1 paragraph 3] ___ ___

23. Has a Maintenance Record (Optional Form 89) Been prepared and maintained for each container/lock/vault door, as applicable when put in use to serve as a permanent record and retained for the service life of the security container/vault door? [EKMS-1(series), Article 520.b (3)] ___ ___

24. Is COMSEC material stored separately from other classified material (e.g., separate container or drawer to facilitate emergency removal or destruction) and segregated by status, type and classification? [EKMS-1(series) Article 520.a(4) and Annex M Paragraph 3] ___ ___

25. When not being used and under the direct control of authorized personnel,

is **all** COMSEC material properly stored?
[EKMS-1(series) Article 520.a(2)] ___ ___

NOTE: Failure to perform the above constitutes a COMSEC Incident. [EKMS-1(series) Article 945.e.]

26. Are software-designed devices in storage at the account level covered as part of the units 3M or other service-specific maintenance program?
[EKMS-5(series), Article 313] ___ ___

NOTE: A list of the devices can be found on the INFOSEC web site under "Hot Topics" Cryptographic Equipment Battery Information (MIP/MRC tab) and (battery information tab).

Commanding Officer: ________________ Manager: _____________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB B

COMSEC SPOT CHECK
EKMS MANAGER/LOCAL ELEMENT ISSUING
(AS APPLICABLE)

MANAGER PERSONNEL

DATE: _______

Yes No

1. Has the Commanding Officer formally designated an EKMS Manager, a minimum of one Alternate, and an EKMS Clerk (as applicable) on an individual Letter of Appointment or Memorandum? [EKMS-1(series) Article 418.a, Annex J] ___ ___

NOTE: Appointment of more than one Alternate Manager to an EKMS Account is recommended. The number of Alternate Managers (beyond the minimum of one) is left to the discretion of the Commanding Officer. [EKMS-1(series) Article 412.a]

2. Are the original copies of current Appointment letter/memorandum retained in the Correspondence/Message File? [EKMS-1(series) Annex J] ___ ___

3. Upon relief of an individual, is the appointment letter/memorandum maintained locally for a minimum of **two years** following the relief of the individual? [EKMS-1(series) Annex T paragraph 2.c] ___ ___

4. Has the command completed the CMS Form 1 and designated properly cleared personnel, one of whom must be the EKMS Manager or Alternate, to drop off/receipt for and courier COMSEC material between their command and CMIO? [EKMS-1(series) Annex H paragraph 1 and 3] ___ ___

NOTE: CMS Form 1 is required **ONLY** if material will be turned in to or picked up from CMIO.

Yes No

5. Does the account have an up-to-date DCS IMT Form-10 on file signed by the current CO? [EKMS-1(series) Articles 405.h.1, 751.b] ___ ___

6. If/when the EKMS Manager is going to be absent for 60 days or more, is the manager relieved of EKMS duties and a new manager formally assigned? [EKMS-1(series) Article 423] ___ ___

7. Does the EKMS Manager ensure that general information concerning the content and intended use of new or revised policies and procedures are brought to the attention of the CO/OIC/SCMSRO and other interested personnel? [EKMS-1(series) Article 455.a] ___ ___

8. Are Alternate(s) kept fully informed of the status of the command’s account so they are at all times fully capable of assuming the EKMS Manager’s duties? [EKMS-1(series) Article 455.d, 460.b] ___ ___

9. Does the EKMS Manager/Alternate conduct at least one spot-check per calendar month (12 per year) on supported Local Elements and ensure that the OIC of remotely located Local Elements are doing the same? [EKMS-1(series) Article 450.i, 1005.a.17] ___ ___

10. Does the EKMS Manager and Alternates use EKMS-3(series) to perform quarterly self-assessments of the primary account and a minimum of one spot check per month and are results of both on file, as required(minimum 12 per calendar year)? [EKMS-1(series) Articles 315.b note, 455.y, 455.z, 1005.a.17, Annex T Para 2.x. ___ ___

> **NOTE:** Questions 12-14 are only applicable in accounts where a Clerk is appointed.

11. Is the EKMS Clerk restricted from having knowledge of/or access to combinations of security containers storing COMSEC keying material and only allowed to maintain TPI

requirements after the COMSEC container has been opened by Manager personnel? [EKMS-1(series), Article 470.c] ___ ___

12. Is the Clerk prohibited from having access to the LMD/KP as either an administrator or operator? [EKMS-1(series) Article 470.c, Annex X paragraph 8] ___ ___

NOTE: Have the Manager or Alternate logon to LCMS under Registration – Operators and verify the clerk (if appointed) is not registered as an administrator (sysadm) or operator (sysopr).

13. Are all receipts, inventories, and destruction reports signed by the clerk, signed as a <u>witness</u> only? [EKMS-1(series) Article 470.b(4)] ___ ___

Commanding Officer: ____________ Manager: _______________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB C

COMSEC SPOT CHECK
EKMS MANAGER

LMD/KP

DATE: ________

Yes No

1. Does the EKMS Manager use LCMS to maintain records for all COMSEC material held by the account? [EKMS-1(series) Article 718.b] ___ ___

2. Is non-COMSEC accountable material being accounted for within LCMS? [EKMS-1(series) Article 706.a.2 (note)] ___ ___

NOTE: The discovery of such constitutes a Non-Reportable PDS. [(EKMS-1(series) Article 1005.a]

3. Is the LMD monitor, KP, and STE arranged to allow the operator to view all displays without obstruction? [EKMS-1(series) Annex X paragraph 12.b] ___ ___

4. Do all EKMS Managers and Alternates have their own unique LCMS/KP Operator IDs? [EKMS-1(series) Annex X paragraph 12] ___ ___

5. Is there a minimum of two LMD/KP System Administrators registered? [EKMS-1(series) Annex X paragraph 9] ___ ___

6. Does the account maintain a KP CIK ID log? [EKMS-1(series) Annex X paragraph 12] ___ ___

NOTE: Failure to maintain a KP CIK Log constitutes a Non-Reportable PDS. [EKMS-1(series) Article 1005.a]

7. Are the PINs and Passwords for each LMD/KP System Administrator and Operator recorded on an SF-700 and properly safeguarded? [EKMS-1(series) Article 520.j.9, Annex X paragraph 12 (NOTE)] ___ ___

8. Have the pre-configured default LCMS SCO password lockout and reset parameters been changed by the Operator and/or System Administrator? (non-compliance with lockout after 3 failed attempts to log on; non-compliance with forced password change every 6 months)? [EKMS-1(series) Article 515.i] ___ ___

NOTE: Failure to reset the password login attempts after changing it to unlock a disabled account constitutes a Reportable PDS [EKMS-1 (series) Article 1005.b]

9. Are System Administrator/Operator PINs/ Passwords changed at minimum of every 6 months and the KP CIK ID and PIN Log updated accordingly? [EKMS-1(series) Article 520.j (7), Annex X paragraph 12] ___ ___

NOTE: Failure to change PINS every six months constitutes a Non-Reportable PDS [EKMS-1(series) Article 1005.a]

10. Does the EKMS Manager ensure that the following routine maintenance functions are performed within the required periodicities?

a. SCO Unix "Root", "/u/usr" and LCMS database backups? [EKMS-1(series) Article 718.d] ___ ___

NOTE: Failure to conduct back-ups/archives constitutes a Non-Reportable PDS. [EKMS-1(series) Article 1005.a]

b. KP Changeover? [EKMS-1(series) Annex X paragraph 12.t.] ___ ___

NOTE: Failure to perform changeovers quarterly constitutes a Cryptographic Incident. [EKMS-1 (series) Article 945.c]

c. KP Rekey? [EKMS-1(series) Annex X paragraph 12.u] ___ ___

NOTE: Failure to perform a KP Rekey at a minimum of annually is a Non-Reportable PDS. [EKMS-1(series) Article 1005.a]

11. Is magnetic media (tapes, floppy diskettes) utilized for backups or archives classified "SECRET" and clearly labeled with the date that the backup or archive, as applicable, was performed? [EKMS-1(series) Article 520.j paragraph (5),(6)] ___ ___

12. Has the Manager ensured the CAD data is current and is updated, as required? [EKMS-1 (series) Articles 455.ad and 602]. ___ ___

13. Has the KP been re-certified in the last 3 years? [EKMS-1(series) Article 1185.e] ___ ___

14. After the replacement KP is received **and operational**, has the old KP been zeroized and sent to CMIO Norfolk VA Broken Copy within 30 days? [EKMS-1(series) Article 1185.e] ___ ___

NOTE 1: EKMS Accounts (other than Cache Accounts) are validated for, and will hold, only one KP for each numbered account.

NOTE 2: Failure to return the old KP within the required timeframe reportable PDS unless the unit **is deployed and unable to enter it into DCS and the account has received a waiver(if so, ask to see the waiver)** [EKMS-1(series) Article 945.e.17, NOTEs 1 and 2]

15. Has the EKMS Manager ensured that the KP has not been used past the re-certification date? [EKMS-1(series) Article 945.c] ___ ___

NOTE: Use of a KP beyond the re-certification date is a COMSEC incident. [EKMS-1(series) Article 945.c]

16. Has the account generated, wrapped and submitted a COAL inventory on a monthly basis? [EKMS-1(series) Article 766.b] ___ ___

NOTE 1: Submarines at sea are exempt from the monthly requirement noted above when on patrol, but will generate a COAL within 30 days prior to going on, and upon return of a patrol. [EKMS-1(series) Article 766.b(4)(b)]

NOTE 2: Unlike a SAIR, Change of Command or Change of EKMS Manager Inventory report, a COAL inventory does not have to be printed and physically completed. [EKMS-1(series) Article 766.b]

Commanding Officer: _______________ Manager:_________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB D

COMSEC SPOT CHECK
EKMS MANAGER/LOCAL ELEMENT ISSUING
(AS APPLICABLE)

RECORDS AND FILES

DATE: ________

1. Does the EKMS Manager maintain a Chronological file that contains the following: [EKMS-1(series) Article 706] ___ ___

a. COMSEC material accounting reports (e.g. receipts, transfers, destruction, conversion, generation, possession and relief of accountability)? ___ ___

b. Accountable Item (A/I) Summary ___ ___

c. Transaction Status Log. ___ ___

d. Inventory reports (e.g., LCMS-operator generated and/or COR-Generated SF 153 Inventory working copies)? ___ ___

e. IMT Form 10 and CMS Form 1 (as required)? ___ ___

f. COMSEC Responsibility Acknowledgment Forms? ___ ___

g. Key Conversion Notices? ___ ___

h. EKMS CF Special Notices? ___ ___

i. Central Facility (CF) Form 1206 (User Representative Registration Request) ___ ___

NOTE: The forms identified above no longer require "wet" signatures and may be submitted and processed electronically. However, they will be printed out and filed in the Chronological file to provide verification during training visits and inspections that they are being updated and maintained due to PCS transfer, retirement, reassignment, etc… to ensure an adequate number of personnel having ordering privileges for the account.

2. Is the EKMS Manager maintaining

a Correspondence and Message file that contains the following: [EKMS-1(series), Article 709]

a. EKMS Account establishment correspondence? ___ ___

NOTE: Mandatory for accounts established after 01 JUL 93.

b. EKMS Manager, Alternate(s), EKMS Clerk, STE Material Control User (MCU) and TPA (as applicable) appointment letters? ___ ___

c. LE (Issuing) and Alternate(s) appointment letters, as applicable? ___ ___

d. COMSEC Incident and PDS reports? ___ ___

e. Correspondence relating to; command allowance, facility approval and authorization to store classified COMSEC material? ___ ___

NOTE: Fixed COMSEC facilities must be certified by the ISIC/IUC prior to storage of classified COMSEC material. The facility must be recertified for storage of classified COMSEC material at least biennially.

f. CMS Assist Visit & Inspection correspondence? ___ ___

g. A list of personnel authorized access to keying material and the LMD/KP? [EKMS-1(series) Article 550.d(1)] ___ ___

h. Spot Check and Self-Assessment Results ___ ___

i. All documentation of training conducted. ___ ___

j. Logs pending destruction (i.e. Audit Trail Review logs, Visitors' logs). ___ ___

3. Does the Directives file contain a copy of each effective command and higher authority directive that relates to COMSEC matters (e.g., guidance for LE personnel, Letters of Agreement and waivers of COMSEC policy and procedures)? [EKMS-1(series) Article 709.c] ___ ___

4. Does the General Message File contain all effective general messages that pertain to

account holdings or COMSEC policy and procedures? (i.e. ALCOM/ALCOMPAC P/ALCOMLANT A) [EKMS-1(series) Article 709.b] ___ ___

5. Is the command maintaining status messages promulgated by the various Controlling Authorities for material held by the account i.e. JCMO 2116XXXXZ, COGARD C4ITSC, etc…? [EKMS-1(series) Art 255, Article 760.a] ___ ___

6. Are file folders clearly marked with the highest classification of the contents and downgrading instructions? [EKMS-1(series) Article 715.d; SECNAV M-5510.36, Articles 6-2, 6-3, 6-27] ___ ___

7. Does each report or file containing classified COMSEC or COMSEC related information include the following statement? [EKMS-1(series) Article 715.d(2)(c)] ___ ___

Derived from: EKMS 1 (series)
Declassify on: 22 September 2028 ___ ___

NOTE: The use of X1 – X8 is prohibited for downgrading/declassifying classified information. Declassification/Downgrading instructions will be in accordance with the CNO Policy ltr Ser N09N2/8U223000 dated 7 Jan 2008 until incorporated into SECNAV M5510.36. For records marked on/after 22 Sep 03, the date shown above reflects 25 years from the last authorized use of X1 – X8.

8. Are inactive COMSEC records, files and logs awaiting expiration of retention periods clearly labeled with the authorized destruction date? [EKMS-1(series) Article 715.c] ___ ___

9. Are KSV-21 cards filled with operational key reflected on the accounts reportable destruction report following loading as "Filled in End Equipment"? [EKMS-1(series) Annex AD paragraphs 17.d and 21.f]? ___ ___

10. Are SF-153 destruction reports submitted to the COR via X.400;

(1) Upon destruction of STE keying material when the KSV-21 card is filled/loaded from the LMD/KP ___ ___

or

(2) When an unused FD (filled by the CF) is loaded into a terminal for the express purpose of zeroizing (destroying) it? [EKMS-1(series) Article 792 and Annex AD paragraph 21] ___ ___

11. Upon receipt of a Key Conversion Notice (KCN), were the following actions completed (only applicable to devices filled with SCIP Modern Key such as Iridium, Sectera, Omni, VIPR, etc. **Not applicable to KSV-21 cards**):[EKMS-1(series) Annex AD paragraph 17.d]

a. Are KCNs processed in LCMS in accordance with the [EKMS-704(series)?] ___ ___

b. Verify that the terminal serial number listed is the serial number of the terminal in which the key was loaded? ___ ___

c. Record keying material as “Filled in End Equipment” in LCMS. [EKMS-1(series) Tab 1 to Annex AD paragraph 12] ___ ___

12. Does the EKMS Account maintain a COMSEC Library consisting of the following manuals/instructions: [EKMS-1(series) Article 721]

a. LMD/KP Operator’s manual, EKMS-704 (series) ___ ___

b. EKMS Intelligent Computer Aided Trainer (ICAT) (also known as the LCMS CBT) ___ ___

c. EKMS Manager JQR ___ ___

d. Local Element CBT ___ ___

e. COMLANTFLT/COMPACFLT/COMUSNAVEURINST C2282.1 (series) – Basic Shipboard Allowance of COMSEC Material. (**Surface ships <u>only</u>**) ___ ___

f. EKMS 1(series) ___ ___

g. EKMS 3(series) ___ ___

h. EKMS 5(series) ___ ___

i. COMDTINST 5510.23 - (**COGARD accounts only**) ___ ___

j. NAG 16(series) ___ ___

k. NAG 53(series) (**Shore-based accounts only)** ___ ___

l. NSA Mandatory Modification Verification Guide (MMVG) ___ ___

m. OPNAVINST 2221.5(series) ___ ___

n. SECNAV M5510.36(series) ___ ___

o. SECNAV M5510.30(series) ___ ___

p. OPNAVINST 5530.14(series) ___ ___

q. SECNAVINST 5040.3(series) ___ ___

r. NAVICPINST 2300.4(series) ___ ___

s. NAVICPINST 5511.24(series) ___ ___

t. OPNAVINST 2221.3(series) ___ ___

u. CJCSI 3260.01(series) (**Required <u>only</u> if account holds SAS material**). ___ ___

v. SDIP 293 (**Required only if the account holds NATO material**). ___ ___

w. AMSG 600 (**Required only if the account holds NATO material**). ___ ___

Commanding Officer: _______________Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB E

COMSEC SPOT CHECK
EKMS MANAGER/LOCAL ELEMENT ISSUING
(AS APPLICABLE)

EKMS ACCOUNT

DATE: ________

Yes No

1. Does the LCMS Accountable Item Summary (A/I Summary) reflect all AL 1, 2, 4, 6 and 7 COMSEC keying material, publications and equipment on charge to the account? [EKMS-1 (series) Article 763.a] ___ ___

2. Are printed copies of the A/I Summary and Transaction Status Log updated, retained and destroyed IAW the following: [EKMS-1 (series) Annex T] ___ ___

TYPE OF COMMAND	FREQUENCY OF PRINTOUTS	RETENTION PERIOD
Submarine	Prior to Deployment	Destroy when replaced with updated versions
Surface or Deployed Mobile Units	Once a month	Destroy when replaced with updated versions
Shore or Non-Deployed Mobile Units	Once every 3 Months	Destroy when replaced with updated versions

NOTE: Each account will close out their Transaction Status Log at the end of each calendar year and retain it on file for 3 years (current year plus two previous years). [EKMS-1(series) Art 724.b, Annex T paragraph 1. (NOTE)]

3. Are SF-153 COMSEC material reports properly completed to include: Transaction Number, Date, Type of Action, Manager/Alternate and Witness Signatures? [EKMS-1(series) Annex U] ___ ___

4. Are receipts for COMSEC material submitted within 96 hours of receipt via the X.400 to

Tier 1? [EKMS-1(series) Article 742.b] ___ ___

NOTE 1: Failure to submit receipts or report of corrupt BETs constitutes a Non-Reportable PDS. [EKMS-1(series) Article 1005.a.15]

NOTE 2: In those instances where the shipments are staggered and reflected on a single transfer report, the 96 hour rule begins when the entire shipment is received. [EKMS-1(series) Article 742.b(2) (NOTE)]

5. Are destruction records being completed for Top Secret and Secret ALC 4 and 7 COMSEC material? [EKMS-1(series) Article 736.b(1)] ___ ___

6. Is destruction of key maintained or issued to an electronic storage device (i.e. DTD, SDS-2000, SKL, TKL) being completed in accordance with EKMS-1(series)? [EKMS-1 (series) Article 540.c (3) (a), Annex AF, Annex Z. ___ ___

7. Is un-issued material that becomes superseded during the month destroyed no later than five working days after the end of the month in which it was superseded? [EKMS-1(series) Article 540.e] ___ ___

NOTE: Failure to destroy superseded material within the required timeframe constitutes late destruction a Non-Reportable PDS. [EKMS-1(series) Article 1005.a]

8. Are the account's end-of-month consolidated destruction reports filed in the Chronological File? [EKMS-1(series) Article 736.b] ___ ___

9. Has the receipt of Two Person Control (TPC) material been reported per CJCSI 3260.01 (series)? [EKMS-1(series) Article 255.d] ___ ___

10. Are pending tracers processed as required? [EKMS-1(series) Article 743] ___ ___

NOTE: Shipment originators that do not receive either a communication or a receipt from the intended recipient within 60 days of the date of the first tracer action constitutes a COMSEC Incident? [EKMS-1(series) Article 743.e, Article 945.e]

11. Does the account report the receipt of corrupt Bulk Encrypted Transactions (BETs) within 96 hours of downloading the BET? [EKMS-1(series) Article 742.d] ___ ___

NOTE: Failure to perform the above constitutes a Non-Reportable PDS. [EKMS-1(series) Article 1005.a]

12. Is Non-Paper COMSEC Material (i.e. Key Tape which is made of Mylar) destroyed by burning or disintegrating in a NSA-Evaluated/authorized destruction device? [EKMS-1(series) Article 540.j.(2)] ___ ___

NOTE: Destruction of COMSEC material by other than authorized means is a Physical Incident. [EKMS-1 1(series) Article 945.e]

13. Are destruction records being completed to document the destruction of all ALC 1, 2 and 6 COMSEC material regardless of its classification? [EKMS-1(series) Article 736.b(1)] ___ ___

NOTE: The absence of destruction reports for material charged to the account must be reported as a Physical Incident. [EKMS-1(series) Article 945.e]

14. Do destruction records clearly identify the command title, account number, short title, edition, reg/serial number, ALC, individual signatures, date of destruction, classification (if applicable), derived from/declassify on instructions (if applicable) short title, edition(s), accounting number, ALC, and date of destruction? [EKMS-1(series) Article 736.a(3); Figures 7-1, 7-2, 7-3] ___ ___

15. Are SF-153 destruction records properly signed and dated by the two individuals who conducted the destruction and are blocks 14 & 16 annotated to indicate the action the SF-153 was used for

(destroyed/witness)? [EKMS-1(series) Article 790.f(1); Figures 7-1-3 paragraph 4, 7-2-2 paragraph 2, 7-3-1 paragraph 2, Annex U] ___ ___

16. Have consolidated destruction records been signed by the either the CO/OIC or SCMSRO? [EKMS-1(series) Annex U paragraph 7.a] ___ ____

NOTE: Missing signature(s) constitutes an incomplete accounting report (Non-Reportable PDS). [EKMS-1 (series) Article 1005.a]

17. Are SAS/TPC destruction reports signed by two members of the SAS/TPC team? [EKMS-1(series) Annex U paragraph 7.b (1)] ___ ___

18. Are only NSA-approved destruction devices used to destroy COMSEC material? [EKMS-1(series) Article 540] ___ ___

Commanding Officer: ______________ Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB F

COMSEC SPOT CHECK
EKMS MANAGER/LOCAL ELEMENT ISSUING
(AS APPLICABLE)

INVENTORIES

DATE: ________

Yes No

1. Has the account conducted an inventory of all COMSEC material in accordance with EKMS-1 (series) Article 766.a, 766.b as reflected below:

a. Semi-annually (twice each calendar year) AL 1, 2, 4, 6, and 7 COMSEC material (including equipment and publications/manuals). ___ ___

b. Change of Command or Consolidated Inventory ___ ___

c. Change of EKMS Manager ___ ___

d. Change of SCMSRO (if applicable) ___ ___

2. Are the results of semi-annual inventories of AL Code 1, 2, and 6 reported to the COR? [EKMS-1(series) Article 766.a.(2)] ___ ___

3. Has the Command submitted a Change of Custodian Inventory Report (CCIR) for a Change of Command, Change of SCMSRO, or Change of EKMS Manager as required? [EKMS-1(series) Article 766.b.(2)] ___ ___

NOTE 1: An inventory will be conducted for activities which are external to the supporting account (LE's), without their own six-digit account who are supported through a Letter of Agreement. [EKMS-1(series) Article 766.a.4 (note)]

NOTE 2: Failure to conduct, document, submit and retain inventories, as applicable within the specified time frames constitutes a Physical Incident. [EKMS-1(series) Article 945.e]

4. Was the SAIR signed by the EKMS Manager, a properly cleared witness, and the CO/OIC/ SCMSRO? [EKMS-1(series) Annex U paragraph 9] ___ ___

NOTE: Three signatures are required for inventories. The absence of one of the three constitutes an incomplete accounting report, a Non-Reportable PDS [EKMS-1(series) Article 1005.a]

5. Was the CCIR conducted for a change of command signed by the outgoing Commanding Officer? [EKMS-1(series) Article 766.a.(3)(a)] ___ ___

6. Are Semi-Annual Inventory reports (SAIRs) being completed and generated via LCMS and sent to the COR via X.400 no later than 30 days after receipt of the COR Request for Inventory Transaction? [EKMS-1(series) Article 766.b (1)(c)] ___ ___

7. Is the COR notified by record message or online reporting upon completion of the physical inventory? This must be accomplished no later than 90 days after the initial request for the inventory is made. [EKMS-1(series) Article 766.b(1)(d)] ___ ___

8. Are completed inventories retained on file for 2 years? (Example: 2007 Chronological files are authorized for destruction 01 Jan 2010). [EKMS-1(series) Annex T] ___ ___

9. If AL 4 or 7 materials are held by the account, is there a separate SF 153 locally generated inventory to document the inventory of that material or has the CO signed all working copies generated for the account and each LE? (Although AL 4 and 7 materials must be inventoried when AL Code 1, 2, and 6 holdings are, the ALC-4 and 7 material is not tracked by the COR But must be accounted for locally? [EKMS-1(series) Article 766.d.(2)] ___ ___

NOTE 1: Working copies of inventory documents must reflect the signatures of the personnel who actually inventoried the material reflected) unsigned required signatures constitute an incomplete accounting report (non-reportable PDS).

NOTE 2: Deployed SSBN’s and SSGN’s which are unable to establish connectivity via X.400 to download required inventories will conduct the inventory on the same interval using a locally generated inventory from LCMS at the earliest possible opportunity and submit a inventory completion message. [EKMS-1(series) Article 766.b.(1)]

10. Are inventory results for ALC-4 and 7 material retained locally for two years? [EKMS-1(series) Articles; 766.a.2, 945.e(16) and Annex T] ___ ____

NOTE 2: If inventories are not on file, as required it cannot be ascertained that the account properly completed the inventory and must be documented as a Physical Incident. **Due to this being a change in retention period from previous policy, such is applicable to inventories conducted Jan 2009 and later only.**

11. Has the account archived LCMS data on a semi-annual basis after each fixed cycle inventory and is archived media labeled, safeguarded and retained as required? [EKMS-1(series) Annex X paragraph 12.s] ___ ___

12. Are the KP REINIT 1 and NAVREINIT 2 keys classified at the level of the accounts HCI and safeguarded appropriately? [EKMS-1 (series) Article 1185.d(1)] ___ ___

NOTE: If not safeguarded based on the classification of the CIKS, report as a Physical Incident. [EKMS-1(series) Article 945.e]

13. Does the account maintain four copies of REINIT 1 and two copies of NAVREINIT 2, and are all reflected on the AIS, as required. [EKMS-1(series) Article 1185.d(3)] ___ ___

NOTE: If the items are not being accounted for in LCMS and reflected on the AIS, report as a Physical Incident. [EKMS-1(series) Article 945.e]

14. Are REINIT 1 and NAVREINIT 2 CIKS properly registered in LCMS as reflected below? [EKMS-1 (series) Article 1185.d(3)(d)]

To verify, in LCMS go to: Registration – COMSEC Material.

a. Are REINIT 1 keys reflected on the AIS as "**AIDS**" and accounted for as **ALC-1?** ___ ___
[EKMS-1(series) Article 1185.d]

b. Are NAVREINIT 2 keys reflected on the AIS as "**Equipment**" and accounted for as **ALC-4?** ___ ___
EKMS-1(series) Article 1185.d]

15. Have discrepancies on the Inventory Reconciliation Status Report (IRST) been communicated to the COR and resolved? [EKMS-1(series) Article 766.b.(1)(e), Annex AK, Paragraph 3] ___ ___

16. Are maintenance and repair kits being inventoried; upon initial receipt; upon installation of modification; during inventories; prior to transfer of the Q(repair kits); and upon destruction? ___ ___
[EKMS-1(series) Annex W]

NOTE: An oral yes is not sufficient for verification of page checks. Randomly open 3 – 5 Q-kits and verify; (a) that an actual inventory is contained in the kit, (b) that the inventory document is signed/dated by the individuals who sight-inventoried the cards and (c) if any card has been removed, that the inventory reflects this and the appropriate documentation is in the kit in place of the removed card.

17. Are page checks conducted on unsealed COMSEC keying material: upon initial receipt; during account inventories; during watch inventories; prior to transfer; and upon destruction? [EKMS-1(series) Annex V] ___ ___

18. Are unsealed maintenance and operating manuals page checked upon initial receipt; after

entry of amendments which change pages (both person entering and person verifying entry); during inventories; prior to transfer; and upon destruction? [EKMS-1(series) Article 815.c] ___ ___

Commanding Officer: _______________Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB G

COMSEC SPOT CHECK EKMS MANAGER/ LOCAL ELEMENT ISSUING (AS APPLICABLE)

STORAGE AND SECURITY

DATE: ________

Yes No

1. Are Two Person Integrity (TPI) requirements maintained for the following COMSEC material: [EKMS-1(series) Article 510.b] ___ ___

a. All Top Secret paper keying material marked or designated CRYPTO? ___ ___

b. Fill Devices containing unencrypted Top Secret key? ___ ___

c. Equipment containing Top Secret key that allows for key extraction? ___ ___

2. Is COMSEC keying material segregated according to status, type and classification? [EKMS-1(series) Annex M paragraph 3.b] ___ ___

3. Does the EKMS Manager and Alternates verify the completeness of COMSEC material received to include checking for signs of tampering and conducting applicable page checks? [EKMS-1 (series) Article 751.d, 754.a – 754.f.] ___ ___

4. Does the EKMS Manager maintain effective and supersession dates for all COMSEC material held by the account? [EKMS-1(series), Article 760.a] ___ ___

5. Does the EKMS Manager maintain an up-to-date copy (electronic or hard copy) of the account's SCMR? [EKMS-1(series) Article 255]. ___ ___

6. For accounts with 500 or more line items, is the required status information entered into LCMS for physical material upon receipt using the Effective Date Tool **and** annotated on the material prior to it being issued to local elements? [EKMS-1(series) Article 760.a]. ___ ___

7. For accounts with less than 500 line items, are effective and supersession dates annotated on the physical COMSEC keying material and COMSEC accountable manuals and publications upon receipt? [EKMS-1(series) Article 760.a] ___ ___

8. Are KSV-21 cards being stored in a GSA approved security container if retained by the EKMS Manager or MC User? [EKMS-1(series) Annex AD (Statement of Responsibility)] ___ ___

9. Have the procedures of EKMS-1 (series) and local command instruction(s) been followed to seal/reseal COMSEC material? [EKMS-1(series) Article 772] ___ ___

NOTE: Segmented material may be considered resealed when placed in a container (e.g., zip lock bag or binder with plastic document protector pages) which will reasonably prevent segments from being lost.

10. If the account has an Iridium phone and sleeve (Short Title: FNBA 20) is the sleeve reflected on the AIS and accounted as an ALC 1 item? [EKMS-1(series) Tab 1 to Annex AD paragraph 3] ___ ___

NOTE (1): Material not reflected on the Accountable Item Summary (AIS) when documentation exists that the material is charged to the account constitutes a Non-Reportable PDS. [EKMS-1(series) Article 1005.a]

NOTE (2): Absence of documentation to indicate the material is charged to the account, the matter would be reported as a Physical COMSEC Incident (found material). [EKMS-1(series) Article 945.e]

11. If an Iridium phone/sleeve (FNBA 20) is held and reflected in LCMS as “issued”, were

proper local custody procedures followed to ensure continuous accountability of the item? [EKMS-1(series) Article 712.a] ___ ___

NOTE: Failure to use LCI documents or their equivalent is a Physical Incident. [EKMS-1(series) Article 945.e]

12. Is Iridium keying material which has been issued/loaded recorded as "Filled in End Equipment" in LCMS? [EKMS-1(series) Article 792, Tab 1 to Annex AD paragraph 12] ___ ___

Commanding Officer: _______________Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER

TAB H

COMSEC SPOT CHECK
EKMS MANAGER

AMENDMENTS AND MODIFICATIONS

DATE: ________

Yes No

1. Are publication corrections made using black or blue/black ink only? [EKMS-1(series) Article 787.g (1)(b)] ___ ___

2. Are pen and ink corrections identified by writing the amendment or correction number in the margin opposite the correction? [EKMS-1(series) Article 787.g(1)(b)(2)] ___ ___

3. If amendment residue is destroyed by a LE are appropriate local destruction records provided to the EKMS Manager? [EKMS-1(series) Article 787.h] ___ ___

4. Is amendment residue destroyed NLT five working days after the entry? [EKMS-1(series) Article 787.h NOTE] ___ ___

NOTE: Failure to destroy amendment residue within the prescribed time frame constitutes "late destruction" which is a non-reportable PDS. [EKMS-1(series) Article 1005.a]

5. Has the person entering the amendment signed and dated the appropriate blanks on the Record of Amendments page? [EKMS-1(series) Article 787.g] ___ ___

6. Has the individual who verified proper entry of the amendment initialed the entry on the Record of Amendments page? [EKMS-1(series) Article 787.g, Figure 7-4] ___ ___

7. If pages were removed, substituted or added, have both the person entering and the person verifying the amendment conducted and

recorded independent page checks of the publication on the Record of Page Checks? [EKMS-1(series) Article 787.g, Figure 7-4] ___ ___

Commanding Officer: _______________Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB I

COMSEC SPOT CHECK
EKMS MANAGER/LOCAL ELEMENT (ISSUING)
(AS APPLICABLE)

ELECTRONIC KEY

DATE: ________

Yes No

1. If the command holds a KVG 83, has it been certified prior to initial use and every two years? [EKMS-1(series) Article 1145.b] ___ ___

2. Is there a certification tag attached to a handle that displays the classification, "CRYPTO" status, date of certification, and name/rank of certifying technician? [EKMS-1 (series) Article 1145.i] ___ ___

3. Are NSA-furnished tamper detection Labels applied to certified/re-certified KVG(s)? [EKMS-1(series) Article 1145.h and 1145.j] ___ ___

NOTE: Serial number discrepancies with applied Tamper Detection labels must be reported as a Physical Incident. [EKMS-1(series) Article 945.e]

4. Have fill devices (KYK-13/KYX-15) containing electronic key been clearly labeled (tagged/marked} with the identity of the key? [EKMS-1(series) Article 1175.a, 1175.b] ___ ___

5. If the account generates or distributes electronic key for OTAD/OTAR/OTAT, are accounting records being maintained and retained for a minimum of 60 days following the date of the last entry on the key generation log? [EKMS-1(series) Article 1182.d (1), Annex T] ___ ___

6. If the account relays or receives electronic key (except for key received

via OTAR), are accounting records being maintained and retained until the key is superseded? [EKMS-1(series) Article 1182.d] ___ ___

7. Does the EKMS Manager or Alternate conduct periodic reviews of OTAT/OTAR accounting logs? [EKMS-1(series) Article 455.k, 1115.c] ___ ___

8. Does the DTD CIK have a tag attached (e.g. via chain) to identify the CIKs classification and serial number? [EKMS-1(series) Annex Z paragraph 9.d] ___ ___

9. Is unrestricted access to Supervisory CIKs or the SSO password, as applicable, limited to only those individuals who are designated in writing and authorized to perform all of the associated privileges? [EKMS-1(series) Annex A, Annex Z paragraph 11.d, Annex AF paragraph 4] ___ ___

10. Does the EKMS Manager or Supervisory User locally account for all DTD CIKs by assigned serial number? [EKMS-1(series) Annex Z paragraph 7] ___ ___

11. For accounts with a Top Secret CIK, is the CIK removed from the DTD or SKL, as applicable and returned to TPI storage when authorized Users are not present? [EKMS-1(series) Annex Z paragraph 10, Annex AF, Paragraph 5.d] ___ ___

NOTE: Otherwise, both CIK and the device must be continually safeguarded according to TPI rules.

12. Have recipients of key issued to either a DTD or SKL signed a local custody document acknowledging receipt of the key? [EKMS-1(series) Article 769.h, Annex Z, paragraph 13.d, Annex AF paragraph 8.f] ___ ___

NOTE: This is applicable whether issued from the LMD/KP or outside of LCMS and also includes fills provided DTD-to-DTD, DTD-to-SKL, or SKL-to-SKL)

13. For **non-watch station** environments, are Supervisory and User CIKs for either the DTD or SKL, as applicable inventoried whenever the account conducts Semi-Annual, Change of EKMS Manager or Change of Command inventory? [EKMS-1(series) Annex Z paragraph 14 a(1), Annex AF paragraph 5.c] ___ ___

NOTE: Local, ISIC, TYCOM policy or the EKMS Manager or Supervisory User may direct more frequent inventories.

14. For **watch station** environments, are the serial numbers of CIKS and associated DTDs visually verified whenever watch personnel change? ___ ___
[EKMS-1(series) Annex Z paragraph 14.b]

15. Is the SKL and user CIK reflected and accounted for on the watch-to-watch inventory? [EKMS-1(series) Annex Z paragraph 14.b (1), (2), Annex AF paragraph 8.f] ___ ___

NOTE: The watch-to-watch inventory will serve as the record of inventory.

16. Is the audit trail data reviewed by the EKMS Manager, Alternate or other properly designated person at a minimum of monthly or more frequently, as required, and are reviews documented in an Audit Review Log? [EKMS-1(series) Article 540.c(3)(a), Annex Z paragraph 17.b, 17.c, Annex AF paragraph 9, Annex AH paragraph 7] ___ ___

NOTE 1: Failure to perform and document Audit Trail reviews constitutes a Physical Incident. [EKMS-1(series) Article 945.e]

NOTE 2: Audit reviews of storage devices possessing Audit Capabilities issued to CMS A&A Teams or school houses where the EKMS Course of Instruction (COI) is facilitated **are not required** unless mandated by local policy or directives.

[EKMS-1(series) Annex AF paragraph 9.c Note 3]

17. Are Audit Trail Review Logs retained for 2 years following the date of last entry? [EKMS-1(series) Annex Z paragraph 17.f(1), Annex T] ___ ___

NOTE: Failure to maintain an Audit Review Log (for 2 years) constitutes a Physical Incident. [EKMS-1(series) Article 945.e]

18. Are monthly backups being performed on the CMWS/DMD PS (if applicable) [EKMS-1(series) Annex AH paragraph 2] ___ ___

NOTE: Failure to perform backups constitutes a Non-Reportable PDS. [EKMS-1(series) Article 1005.a, Annex AH paragraph 2 NOTE]

19. Has unencrypted keymat (red) been loaded or imported into the Tier 3 CMWS/DMD PS (if applicable)? [EKMS-1 (series) Annex AH paragraph 3] ___ ___

NOTE: Performing the above action constitutes a COMSEC Incident. [EKMS-1(series) Article 945.c, Annex AH paragraph 3]

20. Are KSV-21 cards issued following proper local custody procedures ? [EKMS-1(series) Article 712.a, Annex AD paragraph 17] ___ ___

21. Is access to Terminal Privilege Association (TPA) cards restricted to the EKMS Manager, Alternates or other properly designated personnel i.e.(LE Issuing)? [EKMS-1(series) Annex AD paragraph 4] ___ ___

22. Are tamper seals on STE terminals verified at a minimum of semi-annually? [EKMS-1(series) Annex AD paragraph 4] ___ ___

23. Are KSV-21 cards properly accounted for, safeguarded and inventoried. [EKMS-1(series) Annex AD paragraph 16] ___ ___

24. Are COMSEC incident reports promptly

submitted and action taken as required. [EKMS-1(series) Article 450.e] ___ ___

25. Are crypto period extensions, when operationally required and authorized by the CO limited to two hours only? [EKMS-1 (series) Article 450.f] ___ ___

NOTE: If extended beyond 2 hours and such is not authorized by the Controlling Authority, this constitutes a Cryptographic Incident. [EKMS-1(series) Article 945.c]

Commanding Officer: _______________Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB J

COMSEC SPOT CHECK
EKMS MANAGER/LOCAL ELEMENT ISSUING
(AS APPLICABLE)

TRAINING

DATE: ________

Yes No

1. Has the command had a periodic CMS Advice and Assistance (A&A) Training visit between inspection cycles? [EKMS-1(series) Article 315.a] ___ ___

2. Has the command had an EKMS inspection within the past 24 months by command ISIC or IUC? [EKMS-1(series) Article 315.b] ___ ___

3. Have all **USN** military; EKMS Managers, Alternates, LE Issuing, LE Issuing Alternates, EKMS Clerks (if Applicable) and LE user personnel completed the applicable sections of EKMS PQS (NAVEDTRA-43462(series)? [EKMS-1(series) Article 410.j, Article 312] ___ ___

4. Is COMSEC training incorporated, scheduled and accomplished on a monthly basis? [EKMS-1(series) Article 455.f, NOTE] ___ ___

5. Does the EKMS Manager ensure that COMSEC training is properly documented in accordance with command directives and retained? EKMS-1(series) Article 455.f, Annex T] ___ ___

6. Are Emergency Action Plan (EAP)/Emergency Destruction Plan (EDP) training exercises conducted at least annually and documented? [EKMS-1(series) Annex M paragraph 6.d (3)] ___ ___

7. Has the EKMS Manager, Alternate or Tier 3 personnel, as applicable completed CT3/DMD PS Training? [EKMS-1(series) Annex AH 4.b] ___ ___

8. Are maintenance/repair personnel qualified and authorized in writing by the command to perform maintenance on crypto equipment and are DD-1435's documented and on file with the EKMS Manager? [EKMS-5(series) Article 111.b ___ ___

9. Does the EKMS Manager ensure that all equipment meet mandatory modification requirements? [EKMS-1(series) Article 455.u, 757.g; EKMS-5(series) Article 311]] ___ ___

10. Do personnel installing modifications report the entry of modifications and destruction of residue to the EKMS Manager? [EKMS-5(series) Article 310] ___ ___

11. Have LE (Issuing) personnel completed the Computer-Based Interactive Courseware (ICW) and forwarded a copy of the completion certificate to the parent account? [EKMS 1(series) Article 310.b(1)] ___ ___

Commanding Officer: _______________Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB K

COMSEC SPOT CHECK
EKMS MANAGER/LOCAL ELEMENT ISSUING
(AS APPLICABLE)

EMERGENCY ACTION PLAN (EAP)

DATE: ________

Yes No

1. Has the command prepared an Emergency Action Plan (EAP) for safeguarding COMSEC material, in the event of an emergency? [EKMS-1(series) Annex M paragraph 2.a; SECNAV M5510.36, Exhibit 2B] ___ ___

2. Are all authorized personnel at the command/facility made aware of the existence of the EAP? [EKMS-1(series) Annex M paragraph 6.d(2)] ___ ___

3. Does the EKMS Manager maintain the COMSEC portion of the command's EAP? [EKMS-1(series) Article 455.o] ___ ___

4. For commands located within the U.S and its territories, does planning consider natural disasters (e.g., fire, flood, tornado, and earthquake) and hostile actions (terrorist attack, rioting, or civil uprising)? [EKMS-1(series) Annex M paragraph 2.b] ___ ___

5. When planning for natural disaster, does the EAP provide for: [EKMS-1(series) Annex M paragraph 4]

a. Fire reporting and initial fire fighting by assigned personnel? ___ ___

b. Assignment of on-the-scene responsibility for protecting COMSEC material held? ___ ___

c. Protecting material when admitting outside emergency personnel into the secure area(s)? ___ ___

d. Securing or removing classified COMSEC material and evacuating the area(s)? ___ ___

e. Assessing and reporting probable exposure of classified COMSEC material to unauthorized persons during the emergency? ___ ___

f. Completing a post-emergency inventory of COMSEC and Controlled Cryptographic Item (CCI) material and reporting any losses or unauthorized exposure to appropriate authorities? ___ ___

5 For commands located outside the U.S and its territories and deployable units, does planning include both an Emergency Action Plan (EAP) for natural disasters and an Emergency Destruction Procedures (EDP) for hostile actions? [EKMS-1(series) Annex M paragraph 2.c; SECNAV M5510.36, Exhibit 2B Part II paragraph 1] ___ ___

NOTE: Questions 6 – 14 below only apply to EKMS accounts and/or their Local Elements that are located outside the U.S. and its’ territories or deployable units.

6. Does the EKMS account have an Emergency Destruction Plan (EDP) incorporated in their EAP? [EKMS-1(series) Annex M paragraph 2.i] ___ ___

7. Does the EDP identify the chain of authority that is authorized to implement emergency destruction? [EKMS-1(series) Annex M paragraph 5.d (6); SECNAV M5510.36, Exhibit 2B Part II paragraph 4] ___ ___

8. Does the EDP identify individual assignments for destruction? [EKMS-1(series) Annex M paragraph 5.d (5); SECNAV M5510.36 Exhibit 2B PART II paragraph 4] ___ ___

9. Does the EDP include provisions for both PRECAUTIONARY and COMPLETE destruction? [EKMS-1(series) Annex M paragraph 7] ___ ___

10. Are priorities of destruction clearly indicated? [EKMS-1(series) Annex M paragraph 8] ___ ___

11. Does the EDP provide for adequate identification and rapid reporting of material destroyed to higher authority? [EKMS-1(series) Annex M paragraph 10.b ___ ___

12. Are sufficient emergency destruction materials/tools/devices available and in good working order? [EKMS-1(series) Annex M paragraph 5.d, 6.c] ___ ___

13. Are sensitive pages of maintenance manuals prepared for emergency destruction? [EKMS-1 (series) Annex M paragraph 5.e (2)] ___ ___

14. Are weighted canvas bags available to permit jettisoning of COMSEC material (Surface units ships only)? [EKMS-1(series) Annex M paragraph 9.d] ___ ___

Commanding Officer: ______________ Manager: ________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB L

COMSEC SPOT CHECK
EKMS MANAGER/LOCAL ELEMENT ISSUING
(AS APPLICABLE)

LOCAL HANDLING PROCEDURES

DATE: ________

Yes No

1. Has the command promulgated and distributed written instructions and/or extracts of publications to Local Elements (LE) establishing command procedures for handling, accountability, and disposition of COMSEC material. [EKMS-1(series) Article 455.e, Article 721 (NOTE)] ___ ___

2. Has the EKMS Manager promulgated guidance to LEs concerning specific files (reports, messages, and correspondence) the LEs are required to maintain? [EKMS-1(series) Article 703 (NOTE 2)] ___ ___

3. Has the EKMS Manager promulgated instructions/guidance to (Issuing LEs only) on the proper maintenance of their Accountable Item (A/I) Summary? [EKMS-1(series) Article 763.d] ___ ___

4. Have all personnel with access to COMSEC material received a briefing and executed a COMSEC Responsibility Acknowledgment Form? [EKMS-1(series) Article 769.b(2), Annex K] ___ ___

5. Are executed COMSEC Responsibility Acknowledgement Forms retained for 90 days after the individual no longer requires access to COMSEC material, transfers or retires? [EKMS-1(series) Annex T] ___ ___

6. Are all personnel who have access to COMSEC material authorized in writing by the current CO/OIC/SCMSRO? [EKMS-1(series) Article 505.d] ___ ___

7. Is security clearance data for personnel whose duties require access to classified material maintained in JPAS by the Command

Security Manager? [EKMS-1(series) 425, 455.x; SECNAV-M 5510.30A, Article 9-5 paragraphs 2 - 5] ___ ___

NOTE: For USMC, such is documented in the Management Manpower System (MMS). For USCG such is documented in the Personnel Management Information System (PMIS).

8. Does the EKMS manager maintain a local custody file for each LE containing signed, local custody documents for each piece of issued COMSEC material? [EKMS-1(series) Article 712.c] ___ ___

9. Are local custody documents properly filled out, including signatures, short titles, quantity, accounting numbers, AL codes, and date? [EKMS-1 (series) Article 769.c] ___ ___

10. Are local custody documents retained for 90 days after the reflected material has either been destroyed or returned to the EKMS Manager? [EKMS-1(series) Annex T paragraph 2] ___ ___

11. Does the manager ensure that hard copy keying material marked or designated CRYPTO is not issued earlier than 30 days prior to its effective period?[EKMS-1(series) Article 769.e] ___ ___

12. Are Letters of Agreement (LOA) in place for LEs assigned to external commands and are they updated when modified or upon change of command, whichever occurs sooner? [EKMS-1 (series) Article 445, Annex L] ___ ___

13. Prior to releasing COMSEC material to a contractor, has the EKMS Manager ensured the provisions of OPNAVINST 2221.5(series) have been met? [EKMS-1(series) Article 505.g] ___ ___

14. Is the original Letter of Agreement held by the EKMS Manager in the Directives File? [EKMS-1(series) Article 709.c] ___ ___

Commanding Officer: ______________ Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB M

EKMS MANAGER
COMSEC SPOT CHECK

VAULT CHECK-LIST

DATE: ________

Yes No

1. Lock: A combination lock that conforms to the Underwriters' Laboratories, Inc. Standard No. 768, for Group 1R or Group 1. The specific lock model used shall bear a valid UL Group 1R or Group 1 label. ___ ___

NOTE: All vault doors procured after 14 April 1993 must be equipped with a GSA-approved combination lock that meets the requirements Federal Specifications FF-L-2740/2740A. [EKMS-1 Annex N paragraph 2.e (NOTE)]

2. Are shore-based CMS storage vaults equipped with the following minimum safety equipment? [EKMS-1(series) Annex N paragraph 5.a] ___ ___

a. A luminous type light switch?
(**NOTE:** May be painted with fluorescent paint) ___ ___

b. Is emergency lighting installed? ___ ___

c. An interior alarm switch or device? (e.g., telephone, intercom) ___ ___

d. A decal containing emergency instructions on how to obtain release if locked inside the vault? ___ ___

3. If an emergency escape device is considered necessary, have the following minimum requirements been met: [EKMS-1(series) Annex N paragraph 5.b] ___ ___

a. Is it permanently attached to the **inside** of the door and cannot be activated by the exterior locking device, or otherwise accessible from the outside? ___ ___

b. Is it designed and installed so that drilling and rapping the door from the outside will not give access to the vault by activating the escape device? ___ ___

4. If an emergency escape device is not provided, have the following approved Underwriters Laboratories (UL), Inc., devices been installed in the vault: [EKMS-1(series) Annex N paragraph 5.c] ___ ___

a. A UL Bank Vault Emergency Ventilator? ___ ___

b. At least one UL approved fire extinguisher situated in a position near the vault door? ___ ___

NOTE: These provisions are recommended even if an emergency escape device is provided.

5. If the original security integrity of the vault has been degraded in any way, have approved repairs been made? [SECNAV-M 5510.36 Article 10-15] ___ ___

6. Does the vault door unit include a day gate which conforms to the below? [EKMS-1(series) Annex N paragraph 3]

NOTE: This is not a requirement, but is highly recommended.

a. Is the gate of the swing-in hinge type with vertical rods not less than 1/2 inch diameter? ___ ___

b. Is the gate frame made of not **less than** 3/8” by 1 1/2” steel members, and equipped with a locking device arranged to permit locking and unlocking of the gate from the inside? ___ ___

Commanding Officer: _______________Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB N

COMSEC SPOT CHECK
LOCAL ELEMENT

SECURITY

DATE: ________

Yes No

1. Is the space/compartment or vault outwardly identified as “RESTRICTED AREA”? [OPNAVINST 5530.14 (series), Article 210, 218.a.4] [MCO 5530.14(Series) **USMC accounts only**] ___ ___

2. If spaces are not continuously manned, is the main entrance to the COMSEC facility equipped with a GSA approved, electro-mechanical lock meeting Federal Specification FF-L-2740/2740A? [EKMS-1(series) Annex O paragraph 4.b; SECNAV M-5510.36 Exhibit 10A] ___ ___

3. Is only one door used for regular entrance and emergency exits designed so that they can be opened only from inside the COMSEC facility? [EKMS-1(series) Annex O paragraph 4] ___ ___

4. Are windows secured in a permanent manner to prevent them from being opened and screened to prevent inadvertent loss of material, forced entry, or viewing of the space’s interior from an exterior point? (The protection provided to the windows need be no stronger than the strength of the contiguous walls. [EKMS-1(series) Annex O paragraph 5] ___ ___

5. Is the entrance to the COMSEC facility arranged that persons seeking entry can be identified without being admitted to the spaces or being able to view classified material? [EKMS-1(series) Annex O paragraph 4.b] ___ ___

6. Are visitor identification, security clearance and need to know properly verified? [EKMS-1(series) Article 505.b, 550.e; SECNAV M-

5510.30(series) Article 11-1 paragraph 2, 3] ___ ___

7. Is a visitor register in-use, properly maintained and retained for 1 year from the date of the last entry? [EKMS-1(series) Article 550.e(1)(d), Annex T] ___ ___

8. Are the names of individuals with regular duty assignments in the facility, on a formal access list signed by the current CO/OIC/SCMSRO, and has the list been updated whenever the status of an individual changes or at a minimum of annually? [EKMS-1(series) Article 505.d (2)] ___ ___

9. Do all personnel having access to COMSEC material have a clearance equal to or higher than the classification of the material? [EKMS-1(series) Article 505.a] ___ ___

10. Is security clearance data for personnel whose duties require access to classified material maintained in JPAS by the Command Security Manager? [EKMS-1(series) Art 425, 505.a, [SECNAV-M 5510.30A, Article 9-5] ___ ___

NOTE: For USMC, such is documented in the Management Manpower System (MMS); for USCG such is documented in the Personnel Management Information System (PMIS).

11. Have all personnel who have access to COMSEC material been authorized in writing by the current CO/OIC/SCMSRO? [EKMS-1(series) Article 505.d] ___ ___

12. Is **unescorted** access limited to individuals whose duties require such access and who meet access requirements? [EKMS-1(series) Article 550.e(1)(a)] ___ ___

13. In a non-continuously manned COMSEC facility, is a security check conducted and recorded on a SF-701 at the end of the work day? [EKMS-1(series) Article 550.d (3)(b)(b); SECNAV M5510.36 Article 7-11] ___ ___

14. If a COMSEC facility is continuously manned, is a security check conducted at

least once every 24 hours? [EKMS-1(series) Article 550.d(3)(a)] ___ ___

15. Are combinations changed as required; when a new lock is put in-service or replaced, upon transfer or reassignment of personnel who have access, biennially or when compromised)? [EKMS-1(series) Article 515.b] ___ ___

16. Is a Security Container Information Form (SF-700), maintained for **each lock or combination** and placed inside each COMSEC security container? [EKMS-1(series) Article 520.b; SECNAV M5510.36 Article 10-12] ___ ___

17. Are combination records for security containers storing COMSEC material recorded in sealed envelopes and kept on file in a secure central location as designated by the OIC and available to appropriate duty officers for emergency use? [EKMS-1(series) Article 515.e] ___ ___

18. Do storage containers for COMSEC material meet minimum security requirements for the for the highest classification of material stored therein? [EKMS-1(series) Article 520.c, 520.d, 520.e, 520.f; SECNAV M5510.36, Chapter 10] ___ ___

19. Is a Security Container open/closure log (SF-702) maintained for each lock or combination of a COMSEC storage container? [EKMS-1(series) Article 520.b (2)] ___ ___

NOTE: A separate (SF-702) must be used for each combination set on an X-07, X-08 or X-09 lock.

20. Is the exterior of each COMSEC storage container free of external markings, which indicate the classification level of material stored therein? [SECNAV M5510.36 Article 10-1 paragraph 3] ___ ___

21. Has original integrity of COMSEC material storage containers been maintained and are repairs recorded on an OPTIONAL FORM 89 (retained in each container)? [EKMS-1(series) Article 520.b

(3)] ___ ___

22. Are completed SF-701's and SF-702's retained for 30 days beyond the last date recorded? [EKMS-1 (series) Annex T] ___ ___

23. Are all air vents, ducts or any similar openings which breach the walls, floor or ceiling, appropriately secured to prevent penetration? [EKMS-1(series) Annex O paragraph 6] ___ ___

24. Are applicable security controls (e.g., guards, alarms) in place in accordance with SECNAV-M 5510.36 Chapter 10 and [EKMS-1(series) Article 520.a(3)]? ___ ___

25. If a COMSEC facility in a high risk area is unmanned for periods greater than 24 hours, is a check conducted at least once every 24 hours to ensure that all doors are locked and that there have been no attempts at forceful entry. [EKMS-1(series) Article 550.d(3)(c)] ___ ___

26. Are combinations to any one TPI container separated in such a way to prevent any one person from having access to or knowledge of both the "A" and "B" combinations? [EKMS-1(series) Article 515 c.] ___ ___

27. Are combination envelope sealed using transparent lamination or plastic tape? [EKMS-1(series) Article 515.f] ___ ___

a. Names of individuals authorized access to the combinations recorded on the front of the envelope? [EKMS-1(series), Article 515.f] ___ ___

b. Proper classification markings on envelope? [EKMS-1(series), Article 515.d] ___ ___

c. Are the envelopes inspected monthly to ensure they have not been tampered with and the inspection findings documented on a locally generated log? [EKMS-1(series) Article 515.f] ___ ___

28. Is COMSEC material stored separately from other

classified material (e.g., separate container or drawer to facilitate emergency removal or destruction), and segregated by status, type and classification? [EKMS-1(series) Article 520.a(4) and Annex M Paragraph 3] ___ ___

29. When not being used and under the direct control of authorized personnel, are all COMSEC materials properly stored? [EKMS-1(series) Article 520.a(2)] ___ ___

NOTE: Failure to perform the above constitutes a COMSEC Incident. [EKMS 1(series) Article 945.e]

Commanding Officer: _______________Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB O

COMSEC SPOT CHECK

LOCAL ELEMENT

WATCH TO WATCH INVENTORY

DATE: ________

Yes No

1. Does the progressive watch-to-watch inventory list **ALL** COMSEC material held, including accountability for resealed segments/material, KSV-21s, DTDs, SKL's, and associated CIKs? [EKMS-1(series) Article 775.d (1), Annex Z paragraph 14.b, Annex AD paragraph 17 Annex AF paragraph 8.f, Annex AH paragraph 9] ___ ___

NOTE: A watch station is defined as an area which is occupied and operates on a 24-hour day, 7-day a week basis; an 8-hour, 5 day a week basis; or any similar basis. [EKMS-1(series) Article 775.a]

2. Is the material recorded on the progressive watch-to-watch inventory listed by:

a. Short title?

b. Edition?

c. Accounting number (as applicable)?

d. Quantity?

[EKMS-1(series), Article 775.d (2)] ___ ___

3. Is paper keying material inventoried by sighting its short title, edition, accounting number? [EKMS-1(series) Article 775.d (2)] ___ ___

4. If equipment is inventoried by quantity only, does the quantity reflected on the inventory match the quantity held by the work center? [EKMS-1

(series) Article 775.d (7)] ___ ___

NOTE: Query operators for their knowledge of the correct inventory procedures. When inventorying keying material, the destruction documents (CMS-25) must also be reviewed to conduct an inventory properly to ensure all material is either (a) present or (b) destroyed and documented.

5. For COMSEC material that requires TPI, do two appropriately cleared and authorized personnel conduct and sign the watch-to-watch inventory? [EKMS-1(series) Article 775.d] ___ ___

6. Are page checks of unsealed COMSEC material being properly performed? [EKMS-1(series) Articles 757.e.4 775.e] ___ ___

7. Is there a modification record decal plate affixed to all COMSEC equipment that has been modified? [EKMS-1(series) Article 757.g] ___ ___

8. Are superseded watch-to-watch inventory sheets retained at least 30 days after last entry? [EKMS-1(series) Annex T paragraph 2.j] ___ ___

9. If a last copy of a multi-copy key segment was removed from its canister, resealed and is being held until supersession, has the segment been reflected on the watch-to-watch inventory? [EKMS-1(series) Article 775.e (4)] ___ ___

10. Are the Tier 3 CMWS/DMD PS hard drives safeguarded at the Secret level at all times? [EKMS-1(series) Annex AH paragraph 3] ___ ___

Commanding Officer: _______________Manager:________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB P

COMSEC SPOT CHECK
LOCAL ELEMENT

DESTRUCTION

DATE: ________

Yes No

1. Is regularly and irregularly superseded keying material destroyed within 12 hours after the end of the crypto period? [EKMS-1 (series) Article 540.e]

___ ___

2. Is keying material that is being emergency superseded destroyed as soon as possible and within 12 hours of receipt of the emergency supersession notification? [EKMS-1(series) Article 540.f]

___ ___

NOTE: Failure to destroy COMSEC material within the proper time frames outlined is a Non-Reportable PDS. [EKMS-1(series) Article 1005.a]. Exceptions to the 12 hour destruction standard are listed in EKMS-1 (series) Article 540.

3. Are only NSA approved devices used for the routine destruction of COMSEC material? [EKMS-1 (series) Article 540]

___ ___

NOTE: Failure to use either approved destruction devices or methods constitutes a COMSEC Incident. [EKMS-1(series) Article 945.e]

4. Are destruction records being completed to document the destruction of all ALC 1, 2 and 6 COMSEC material regardless of its classification? [EKMS-1(series) Article 736.b(2)]

___ ___

5. Prior to destroying any COMSEC material, is the status, short title, and accounting data for each item of material being destroyed verified, validated, and sighted by both personnel performing the destruction?

[EKMS-1(series) Article 790.a] ___ ___

6. Is the short title(s), edition, and reg/serial number read off by the 1st person performing the destruction and verified by the 2nd person and then the process reversed to verify the material against the destruction documents used? [EKMS-1(series) Article 790.c] ___ ___

7. Are destruction devices and the surrounding area inspected afterward to ensure that destruction was complete and that no material escaped during the destruction process? [EKMS-1(series) Article 790.g (2)] ___ ___

8. Are empty keytape canisters punctured on both sides of the canister and verified empty before disposal? [EKMS-1(series) Article 540] ___ ___

9. Do local destruction records for segmented COMSEC material reflect the below? [EKMS-1(series), Figure 7-1, 7-2, 7-3]

a. Short title and complete accounting data (edition, reg/serial number, ALC? ___ ___

b. Date of destruction? ___ ___

c. Signatures of the two persons conducting the destruction? ___ ___

d. Marked “CONFIDENTIAL (When filled in)”? ___ ___

e. Downgrading/Declassification markings?

Derived from: EKMS 1 (series)
Declassify on: 22 September 2028 ___ ___

10. Is there only one copy of a short title, edition, and accounting number recorded on the CMS 25 or locally prepared segmented destruction document? [EKMS-1(series) Figure 7-1-3 paragraph 8] ___ ___

11. If keying material was unintentionally removed from its protective packaging prior to its effective period was the material

resealed and the associated destruction document annotated to explain the removal? [EKMS-1(series) article 772.d] ___ ___

Note: Except as indicated in EKMS-1(series) Article 769.g Note 1, premature extraction is a non-reportable. Whether done unintentionally or intentionally to support an operational requirement, premature extraction **MUST** be recorded on the local destruction record (CMS-25) for the material.

a. A statement that the keytape segment(s) was unintentionally removed? ___ ___

b. The date of the unintentional removal? ___ ___

c. Identity of the keytape segment(s) actually removed? ___ ___

d. Signatures of the individuals who removed the key? ___ ___

Commanding Officer: ______________ Manager_______________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB Q

COMSEC SPOT CHECK
LOCAL ELEMENT

COMSEC PROCEDURES AND HANDLING

DATE: ________

Yes No

1. Has the command promulgated and distributed written instructions and/or publication extracts establishing command procedures for handling, accountability, and disposition of COMSEC material? [EKMS-1 (series) Article 455.e, 721 (NOTE)] ___ ___

2. Are required files (reports, messages, correspondence) maintained by the LE as directed by promulgated guidance from the EKMS Manager? [EKMS-1(series) Article 703 (NOTE 2)] ___ ___

3. Are local custody documents properly filled out including; short titles, editions, reg/serial numbers, quantity, AL codes, signature data and date(s), as applicable? [EKMS 1(series) Article 769.c] ___ ___

4. If amendment residue is destroyed by local element personnel, are appropriate local destruction records provided to the EKMS Manager? [EKMS-1(series) Article 787.h] ___ ___

5. Are pen and ink corrections completed only in black or blue-black ink and identified in the margin, opposite their entry? [EKMS-1 (series) Article 787.g] ___ ___

6. Is each pen and ink correction identified by writing the correction number in the margin opposite the correction? [EKMS-1(series) Article 787.g] ___ ____

7. Has the individual entering a correction signed and dated the ROA page of the publication certifying that he/she has

entered the change? [EKMS-1(series) Article 787.g] ___ ___

8. Has the individual who verified proper entry of the correction initialed the entry on the Record of Amendments page? [EKMS-1(series) Article 787.g] ___ ___

9. Have both the person entering the correction and the person verifying the correction conducted a page check of the publication, and recorded this on the Record of Page checks page? [EKMS-1(series) Articles 787.g(4),787.g(5)] ___ ___

10. Has all unsealed COMSEC material been sealed/resealed in accordance with EKMS-1 (series) and local command instructions? [EKMS-1(series) Article 772] ___ ___

NOTE: Unsealed segmented material is considered resealed when placed in a container (e.g. zip lock bag or a binder with plastic document protector pages which reasonably prevent the segments from being lost or misused), or sealed in an opaque envelope using the alternative sealing method. [EKMS-1 Article 772.h]

11. Does the local custody file contain effective signed local custody documents for all issued material? [EKMS-1(series) Article 712] ___ ___

12. Do local custody documents (i.e., SF 153, or locally prepared equivalent), contain the <u>minimum</u> required information? [EKMS-1(series) Article 769.c(1)] ___ ___

13. Are local custody documents being maintained on file for 90 days after supersession? [EKMS-1 (series) Annex T paragraph 2.a] ___ ___

14. Have inventories for a NON-WATCH STATION environments been conducted and recorded on a local custody issue document in accordance with EKMS-1? [EKMS-1(series) Article 778.c] ___ ___

15. Are required page checks being accomplished as follows: [EKMS-1(series) Article 757,775.e,

Annex W]

a. Unsealed COMSEC keying material. Upon initial receipt; during account and watch inventories; and prior to destruction? ___ ___

b. Resealed keying material. During Fixed-Cycle and Change of EKMS Manager inventories; and upon destruction? ___ ___

c. Unsealed maintenance and operating manuals. Upon initial receipt; after entry of an amendment which changes pages; during Semi-Annual (Fixed-Cycle) and Change of EKMS Manager inventories; and upon destruction? ___ ___

d. Unsealed amendments. Upon initial receipt; after entry of amendment which changes pages; during Fixed-Cycle and Change of EKMS Manager inventories; during watch inventories; and upon destruction? ___ ___

16. Are page check discrepancies reported to the account EKMS Manager or Alternate? [EKMS-1(series) Article 775.f, 778.d] ___ ___

17. Are keytape canisters free of locally applied labels (including removal of the NSA applied bar code label)? [EKMS-1(series) Article 760.e NOTE, 760.f] ___ ___

Commanding Officer: ______________ Manager: ________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB R

COMSEC SPOT CHECK
LOCAL ELEMENT

ELECTRONIC KEY

DATE: ________

Yes No

1. If the Local Element has a KVG 83 installed, is its certification current (prior to initial use and every two years)? [EKMS-1(series) Article 1145.b] ___ ___

2. Has a certification tag been attached to the handle on the KVG 83 that displays the classification, "CRYPTO" status, date of certification, and name/rank of certifying technician? [EKMS-1(series) Article 1145.i] ___ ___

3. Have fill devices (KYK-13/KYX-15) containing electronic key been clearly labeled (tagged/marked} with the identity of the key it contains? [EKMS-1(series) Article 1175.a, 1175.b] ___ ___

4. Has NSA-furnished tamper detection labels been applied to certified/recertified KVG(s)? [EKMS-1(series) Article 1145.h, 1145.j] ___ ___

NOTE: Serial number discrepancies with applied Tamper Detection labels must be reported as a Physical Incident. [EKMS-1(series) Article 945.e]

5. If the COMSEC facility has certified KVG(s) equipment installed for operational use, is the equipments "Dutch Doors" double-locked or protected under **no-lone zone (NLZ)** procedures? [EKMS-1(series) Article 1145.k] ___ ___

6. If the element generates or sends electronic key (OTAD/OTAR/OTAT), are accounting records being maintained and retained for a minimum of 60 days following the date of the last entry on the key generation log? [EKMS-1(series) Article 1182.d

(1), Annex T] ___ ___

7. If the element relays or receives electronic key (except for key received via OTAR), are accounting records being maintained and retained until the key is superseded? [EKMS-1(series) Article 1182.d] ___ ___

8. In a watch environment, are KSV-21 cards reflected on the watch to watch inventory? [EKMS-1(series) Annex AD paragraph 17.b] ___ ___

9. Do the DTD CIKs have a tag attached (e.g. via chain) to identify the classification of the CIK and its’ serial number? [EKMS-1 (series) Annex Z paragraph 9.d] ___ ___

10. Is the Audit Trail data reviewed or submitted to the EKMS Manager/Alternate at a minimum of once per month or when the Audit Trail icon illuminates, or sooner as required and documented in the Audit Review Log? [EKMS-1(series) Article 540.c(3)(a), Annex Z paragraph 17.b, 17.c, Annex AF paragraph 9, Annex AH paragraph 7] ___ ___

NOTE 1: Failure to perform and document Audit Trail reviews monthly is a Physical Incident. [EKMS-1(series) Article 945.e]

NOTE 2: Audit reviews of storage devices possessing Audit Capabilities issued to CMS A&A Teams or school houses where the EKMS Course of Instruction (COI) is facilitated are **not required** unless mandated by local policy or directives. [EKMS-1(series) Annex AF paragraph 9.c Note 3]

11. Are monthly backups being conducted and documented on the CMWS/DMD PS (as applicable) [EKMS 1(series) Annex AH paragraph 2] ___ ___

NOTE: Failure to perform backups on the CMWS/DMD PS is a Non-Reportable PDS. [EKMS-1(series) Article 1005.a, Annex AH Paragraph 2 NOTE]

12. If the COMSEC facility has keyed crypto equipment from which Top Secret key may be

extracted, is the equipment protected under TPI? [EKMS-1(series) Article 510.d, e] ___ ___

13. Are all COMSEC fill devices loaded with Top Secret key, and/or unloaded COMSEC fill devices in an environment containing keyed crypto-equipment, from which Top Secret key may be extracted, being protected under TPI? [EKMS-1(series) Article 510.d] ___ ___

14. Are software-designed devices covered as part of the units 3M or other service-specific maintenance program? [EKMS-5(series) Article 313] ___ ___

NOTE: A list of the devices can be found at: https://infosec.navy.mil/crypto/

Commanding Officer: _______________ Manager:_________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.

TAB S

COMSEC SPOT CHECK
LOCAL ELEMENT

EMERGENCY ACTION PLAN (EAP)

DATE: ________

Yes No

1. Has the command prepared an Emergency Action Plan (EAP) for safeguarding COMSEC material, in the event of an emergency? [EKMS-1(series) Annex M paragraph 2.a (3) (d); SECNAV M5510.36, Exhibit 2B] ___ ___

2. For commands located within the U.S and its territories, does planning consider natural disasters (e.g., fire, flood, tornado, and earthquake) and hostile actions (terrorist attack, rioting, or civil uprising)? [EKMS-1(series) Annex M paragraph 2.b] ___ ___

3. Are all authorized personnel at the command/facility made aware of the existence of the EAP? [EKMS-1(series) Annex M paragraph 6.d(2)] ___ ___

4. For commands located outside the U.S and its territories and deployable units, does planning include both an Emergency Action Plan (EAP) for natural disasters and an Emergency Destruction Procedures (EDP) for hostile actions? [EKMS-1(series) Annex M paragraph 2.c; SECNAV M5510.36, Exhibit 2B Part II paragraph 1] ___ ___

NOTE: Questions 5 - 15 below only apply to EKMS accounts and/or their Local Elements that are located outside the U.S. and its territories or deployable units.

5. Does the EDP identify the chain of authority that is authorized to implement that emergency destruction?[EKMS-1 (series) Annex M paragraph 5.d (6); SECNAV M5510.36, Exhibit 2B Part II paragraph 4] ___ ___

6. Does the EDP identify individual assignments for destruction? [EKMS-1(series) Annex M paragraph 5.d (5); SECNAV M5510.36, Exhibit 2B Part II paragraph 4] ___ ___

7. Does the plan include provisions for PRECAUTIONARY and COMPLETE emergency destruction? [EKMS-1(series) Annex M paragraph 7] ___ ___

8. Are priorities of destruction clearly indicated and the COMSEC material separated by classification and status in order to facilitate emergency destruction? [EKMS-1(series) Annex M paragraph 8] ___ ___

9. Are all personnel familiar with all the duties of each assignment to facilitate changes in assignments if necessary? [EKMS-1(series) Annex M paragraph 6] ___ ___

10. Are EAP/EDP training exercises conducted and documented annually and documented? [EKMS-1(series) Annex M paragraph 6] ___ ___

11. Are devices and facilities for the emergency destruction of COMSEC material readily available and in good working order? [EKMS-1(series) Annex M paragraph 5.d and 6.c] ___ ___

12. Are the sensitive pages of KAMs prepared for **ready** removal (i.e., upper left corner clipped), and are the front edges of the covers/binders marked with a distinctive marking (i.e., red stripe)? [EKMS-1(series) Annex M paragraph 5.e(2)(a)] ___ ___

13. Does the EDP stress that accurate information concerning the extent of emergency destruction is second in importance only to the destruction of the material itself? [EKMS-1(series) Annex M Paragraph 10.a] ___ ___

14. Are document sinking bags available in sufficient quantity and in good condition

to permit jettison of COMSEC material? [EKMS-1 (series) Annex M paragraph 9.d] ___ ___

NOTE: #14 above is only applicable to surface units [EKMS-1(series) Annex M paragraph 9.d]

15. If the LE deploys in aircraft, does the plan cover specific actions to be followed in the aircraft? [EKMS-1(series) Annex M paragraph 9.c] ___ ___

Commanding Officer: ___________ Manager: ________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER.