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

COMSEC MANAGEMENT FOR COMMANDING OFFICER'S HANDBOOK

08 May 2017

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

2250
Ser N5
08 May 17

From: Commanding Officer, Naval Communications Security Material System

Subj: COMSEC MANAGEMENT FOR COMMANDING OFFICER'S HANDBOOK LETTER OF PROMULGATION

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

2. BACKGROUND. Experience has shown command involvement, oversight and engagement in COMSEC matters enhances mission readiness, security and results in fewer COMSEC incidents and Practices Dangerous to Security (PDS's).

3. INTRODUCTION.

a. This handbook is intended to provide the Commanding Officer (CO), Perspective CO (PCO), Officer-in-Charge (OIC) and Staff CMS Responsibility Officer (SCMSRO) with a basic understanding of COMSEC account management and responsibilities. It does not provide the scope or level of detail found in the Electronic Key Management System EKMS-1(series) or EKMS-1(series) Supp-1 and is not intended for use by COMSEC Account Managers for account management.

b. A copy of this handbook and additional information of interest to CO's, OIC's and SCMSRO's can be found on the NCMS SIPRNET Collaboration At-Sea (CAS) portal located at (lowercase): http://www.uar.cas.navy.smil.mil/secret/navy/39/site.nsf or the INFOSEC Web Site located at: https://infosec.navy.mil

c. Account Managers can use individual tabs contained herein for the purpose of conducting monthly spot checks; semi-annual self-assessments will be conducted using EKMS-3(series).

d. It is recommended, the most recent version of this

Subj: COMSEC MANAGEMENT FOR COMMANDING OFFICER'S HANDBOOK LETTER OF PROMULGATION

handbook be included in the command turnover file/folder and maintained in the CO's, OIC or SCMSRO's personal library of reference material.

e. Throughout this document where used, the term "Commanding Officer" applies to CO's, OICs and SCMSROs. The term COMSEC account pertains to an EKMS or KMI account and unless specifically identified otherwise, the term Account Manager pertains to an EKMS Manager or KMI Operating Account Manager (KOAM).

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

5. SCOPE. The information contained herein 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. The COMSEC Management for CO's handbook is effective upon receipt supersedes any earlier dated version.

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).

LECOUNTE.JAMES.A.1062461426 Digitally signed by LECOUNTE.JAMES.A.1062461426
Date: 2017.05.18 07:26:16 -04'00'

J. A. LECOUNTE

LIST OF EFFECTIVE PAGES

PAGES	**PAGE NUMBERS**	**EFFECTIVE**
FRONT COVER	(UNNUMBERED)	ORIGINAL
LETTER OF PROMULGATION	01 THRU 02	ORIGINAL
LIST OF EFFECTIVE PAGES	i	ORIGINAL
RECORD OF AMENDMENTS	ii	ORIGINAL
RECORD OF PAGE CHECKS	iii	ORIGINAL
TABLE OF CONTENTS	iv THRU vi	ORIGINAL
SECTION I	1 THRU 7	ORIGINAL
SECTION II	1 THRU 9	ORIGINAL
SECTION III	1 THRU 2	ORIGINAL
SECTION IV	1 THRU 2	ORIGINAL
SECTION V	1 THRU 3	ORIGINAL
TAB A	A1 THRU A26	ORIGINAL
TAB B	B1 THRU B17	ORIGINAL

RECORD OF AMENDMENTS

Identification of Amendment	Date Entered (YYMMDD)	By Whom Entered (Signature, Rank or Rate, Command Title)

RECORD OF PAGE CHECKS

DATE CHECKED	CHECKED BY SIGNATURE, RANK/RATE, COMMAND TITLE)
05/08/17	PHILLIPS.MILLARD.J.III.1114056975 M. J. PHILLIPS, CIV, NCMS, N5A Digitally signed by PHILLIPS.MILLARD.J.III.1114056975 Date: 2017.05.17 16:14:23 -04'00'

COMSEC MANAGEMENT FOR COMMANDING OFFICER'S HANDBOOK TABLE OF CONTENTS

SECTION I

1. GENERAL ADMINISTRATION

a. General. The 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).

Appointment of a SCMSRO must be in writing; the SCMSRO 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, in writing an active duty officer in charge (OIC) to sign routine EKMS reports in his/her absence as "acting." The CO must, at the first opportunity 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 appoint the supporting I&I as the SCMSRO for routine CMS matters.

2. COMSEC 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. The CMCS was established to account for, control and distribute COMSEC material.

At the unit level, COMSEC material is accounted for, tracked and managed using the Local Management Device Key Processor (LMD/KP). or the Management Client Advanced Key Processor (MGC/AKP).

b. National Security Agency (NSA). The National Security Agency (Tier 0) serves as the executive agent for developing and

implementing national level policy affecting the control of COMSEC material, and 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. Central Facility (CF). The CF operates as part of the NSA and 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 or must be generated by Tier 0 for other reasons. 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). Overall responsibility and authority for implementation of National COMSEC policy within the DON. The Head, Navy Information Assurance (IA) Branch is the COMSEC resource sponsor and is responsible for consolidating the COMSEC programming, planning and implementation of policy and technical improvements.

f. Department of the Navy Chief Information Officer (DON CIO). As the Executive Agent, DON CIO is overall responsible for DON COMSEC policy and oversight

g. Headquarters Marine Corps (HQMC). HQMC C4 CY serves as COMSEC resource sponsor for the Marine Corps. The department functions as the USMC Service Authority and coordinates with CNO, COMNAVCYBERFOR, and NCMS to establish, promulgate, and oversee COMSEC account management matters unique to the Marine Corps. The C4/CY is the focal point for requirements and administration for all Marine Corps COMSEC accounts.

h. Commander, U.S. Coast Guard C4IT Service Center, Information Assurance Branch (C4ITSC-BOD-IAB): Acts as the USCG Service Authority (SA), exercises overall authority for USCG COMSEC matters and serves as the USCG Program Manager and Principal Agent for the USCG COMSEC Program and also functions as

the USCG; Closing Action Authority, Command Authority (CA) and USCG ISIC.

i. Naval Communications Security Material System (NCMS). Administers the DON COMSEC program, is the Service Authority and serves as the Central Office of Record (COR) for DON Tier 1 for Tier 2 accounts. Additional duties and responsibilities can be found in Article 120 to EKMS-1(series).

j. Controlling Authority (CONAUTH). A "CONAUTH" is defined as 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. The CONAUTH is responsible for evaluating COMSEC incidents and authorizing the issuance, destruction and transfer of COMSEC material under their cognizance.

k. Immediate Superior in Command (ISIC)/Immediate Unit Commander (IUC). The ISIC/IUC is responsible for the administrative oversight of all COMSEC matters and the conduct of biennial COMSEC COR Audit of their subordinate commands.

l. Commanding Officer (CO)/Staff CMS Responsibility Officer (SCMSRO) / Officer in Charge (OIC). The CO, OIC or SCMSRO, as applicable is responsible for the proper operation and administration of the command's COMSEC account.

m. Command Authority (CA/CMDAUTH). The individual responsible for the management of Modern Key ordering privileges. Normally, the ISIC or Type Commander (TYCOM) performs CA/CMDAUTH responsibilities for their subordinate units.

n. COMSEC Account Manager. The CO must appoint, in writing, one COMSEC Account Manager and a minimum of one alternate. It is recommend if the accounts Highest Classification Indicator (HCI) is Top Secret two additional properly cleared and trained alternates be appointed for redundancy during periods of leave, TDY, etc… Alternates must be as familiar with the account and share equally responsibility for the proper management and administration of the EKMS account. The individual must be a U.S. Military member or Government Civil Service employee.

o. 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. More than one account manager must have ordering privileges for modern key required by the unit to prevent potential mission impact.

p. Client Platform Administrator (CPA). The CPA is only applicable to units which have transitioned to the KMI and is responsible for System Administration of the KMI Management Client referred to as the MGC. The CPA must be appointed in writing, have a minimum SECRET security clearance, current within 10 years and meet the designation and training requirements set forth in Chapters 4 and 6 to EKMS-1B Supp-1.

q. Client Platform Security Officer (CPSO). The CPSO is only applicable to units which have transitioned to the KMI and is responsible for security monitoring, including the review of audit data associated with the MGC. To minimize manpower requirements, it is recommended the units Information System Security Manager (ISSM) of Information System Security Officer (ISSO) be appointed to fulfill the duties of the CPSO as they are already required to have a Single-Scope Background Investigation (SSBI) current within (5) years and be Information Assurance Technician (IAT) Level 1 or higher certified per DOD 8570.01M.

> **Note:** Due to role restrictions set forth in National policy, the KOAM and CPA cannot serve concurrently as the CPSO. A KOAM or Alternate may serve concurrently as the CPA if the incumbent meets the training requirements mentioned in subparagraph "p" above.

r. Account Clerk. An individual designated in writing by the CO who assists the COMSEC Account Manager and Alternate(s) with routine administrative account matters. Appointment of a Clerk is not mandatory but is at the discretion of the CO. Additional information regarding appointment of a Clerk can be found in Articles 170 and 414 to EKMS-1(series).

> **Note:** As stipulated in the Security Doctrine for the LMD/KP and MGC/AKP, access to the LMD/KP or MGC/AKP is restricted to personnel who have received formal training and are assigned as an Account Manager or Alternate.

s. Local Element (LE). There are two variants of Local Elements: LE (Using) and LE (Issuing). The primary difference between LE (Using) and LE (Issuing) is that LE Using (Users) are normally work centers within the same organization in which the account resides and which receive COMSEC material from their activities COMSEC account for use in their respective division or work center. Typically, these entities operate on a watch-to-watch basis and do not further issue COMSEC material on a Local Custody basis. Examples include Radio, CIC, SATCOM, Tech Control, etc…

LE (Issuing) receives material from parent COMSEC account or another established account to issue material on a local custody basis. The issuance of COMSEC material from an established COMSEC account to either LE Users or LE Issuing which are not part of the organization owning the COMSEC account (external) must be established and supported through a formal Letter of Agreement per Article 445 to EKMS-1(series).

LE (Issuing) units are required to properly account for, store, issue, inventory, destroy and safeguard COMSEC material provided to them. They are required to create and retain required accounting documentation (e.g., LCI and local destruction records). LE (Issuing) personnel must be appointed in writing and meet the designation requirements outlined in Article 414 to EKMS-1(series). Issuing LEs must be attached to the command or unit they will be servicing with COMSEC material.

t. Witness. Any properly cleared U.S. Government employee or 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.

> **Note:** For contractor personnel, blocks 10 and 11 to the DD-254 must state access to COMSEC material is required in fulfillment of the Statement of Work (SOW). Per the NISPOM, NSA/CSS 3-16 and CNSSP-14 access is restricted to the SECRET level for contractor personnel when an Interim Top Secret is issued to contractor personnel.

3. DUTIES AND RESPONSIBILITIES.

a. Staff CMS Responsibility Officer (SCMSRO). 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 staff officer (O-4 (or selectee)/GS-12, Pay Band 2, or above). Officers not meeting the above requirement may not designate a SCMSRO. A SCMSRO may exist at a command with an account or LE command if headed by a flag or general officer or an officer occupying such billet. With exception of biennial COR Audit, a SCMSRO who meets the requirements stated herein and has been appointed in writing by a flag or general officer may act and fulfill the ISIC responsibilities found in EKMS-1(series).

(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 duties of the COs/OICs reflected below.

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

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

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

(b) Appoint, in writing, qualified, properly cleared and responsible individuals as Account Manager and Alternates, Local Element (Issuing), and, if desired, a 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 COMSEC Account Manager 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 Personnel Qualification Standards (PQS) (NAVEDTRA 43462 {series}) by USN military personnel serving as; COMSEC Account Managers, Alternates, Local Elements (both issuing and using and Clerks, as applicable.

(g) Ensure COMSEC incidents are reported within the timeframes set forth in Article 960 to EKMS-1(series).

(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 at a minimum of quarterly on the COMSEC account in accordance with Article 450 to EKMS-1(series) (See Section IV).

(j) Receive debriefings from COR Auditors.

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

(l) Ensure appointments of Account Managers is documented in service records or position descriptions.

(m) Ensure an Emergency Action Plan (EAP)/Emergency Destruction Plan (EDP) is established and tested at a minimum of annually. The plan must provide for the protection and/or destruction of COMSEC material during emergency conditions.

(n) Ensure an inventory of all COMSEC material is conducted on the following occasions:

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

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

(3) Semi-Annually

(4) When a COMSEC account is disestablished.

Note: Further information related to inventories and signature requirements can be found in EKMS-1(series).

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

SECTION II

1. **COMSEC ADMINISTRATION**

a. Appointment Letter/Memorandum. An administrative **document, signed by the current CO, formally designating** individuals to duties as a; COMSEC Account 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.

Due to the required retention period, individuals must be appointed on individual appointment letters. At the discretion of the CO, LE Using personnel 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 are assigned in lieu of an individual appointment/designation letter. If an access list is used it must be updated at a minimum of annually or more frequently, as required.

b. EKMS Library. Each COMSEC account is required to maintain a COMSEC library consisting of the publications reflected in Article 721 to EKMS-1(series), Annex C to EKMS-1 Supp-1 and the COMSEC Library Spot Check contained herein. However, the following primary policy documents should be periodically reviewed by the Commanding Officer for additional guidance not contained herein.

(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 and KMI COR Audit Manual" establishes qualification standards for COR Auditors and prescribes minimum standards for conducting COR Audits. It is provided to help the Manager ensure the account is effectively managed 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-1(series) Supp-1. DON KMI Policy Manual. This publication provides guidance to COMSEC Account Managers at units

which have transitioned to the KMI.

c. CMS Form 1. A locally prepared form required for over-the-counter services with CMIO Norfolk. The form must be updated annually or upon change of command, whichever occurs sooner. The CMS Form 1 (Figure-2) must be submitted on command letterhead or an official message; guidance can be found in Annex H to EKMS-1(series).

d. USTRANSCOM IMT Form 10. To deliver or receipt for material from the Defense Courier Service (DCS), the units must have an up-to-date USTRANSCOM Form 10 on file with the DCS station. DCS operates as part of the U.S. Transportation Command and is not under the purview of NCMS. The DCS Customer Service manual can be found here.

e. User Representative (UR) Registration Form. The Central Facility (CF Form 1206) must be prepared by the command, submitted to and approved by the organizations Command Authority (CA) to permit the ordering of modern keying material. At a minimum, the COMSEC Account Manager and (1) one or more alternates must have ordering privileges. Modern key is not supplied or automatically distributed, it must be ordered by a person possessing the applicable privileges.

f. Command Handling Instruction. Each command holding COMSEC material must prepare a local handling instruction to delineate how COMSEC material will be handled, stored and safeguarded. Emphasis must be placed on material accountability, Two-Person-Integrity (TPI) requirements, security, the timely identification and reporting of COMSEC incidents or PDS's and additional or more stringent requirements imposed at the discretion of the local CO. A copy of the instruction must be provided to all Account Managers and LE personnel.

g. Command Security Procedures. Local procedures must be established for the timely identification of potentially significant changes in life-style, financial status, or disciplinary problems involving personnel authorized access to COMSEC material. If detected, such changes must be reported to the Command Security Manager or the Special Security Officer (SSO), as applicable per SECNAV M5510.30.

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

activities located within the U.S and its territories the plan should consider both 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 can be found in Annex M to EKMS-1 (series).

i. Letter of Agreement (LOA). A LOA is used to establish and maintain a COMSEC support agreement between Commanding Officers when an organization does not have its own account to satisfy mission requirements. LOA's are not required for one-time support but are required for standing support arrangements. Letters of Agreement remain in effect until modified or the support is no longer required. LOAs/MOUs will be reviewed at a minimum of triennially. It is highly recommended within 90 days of assuming command or as soon as practical thereafter the incoming CO review existing COMSEC-related LOAs/MOUs. A sample LOA can be found in EKMS 1 (series).

2. **RESOURCE ASSISTANCE.** The below services and resources exist and should be consulted when necessary to prepare for formal COR Audits or obtain clarification or guidance on matters related to COMSEC policy or procedures. These include:

a. COMFLT/TYCOM/ISIC/CMS COR Audit Training Team: When in doubt about a COMSEC matter, the COMSEC Account Manager should consult with the ISIC, TYCOM, FLTCDR or servicing CMS COR Audit Team. A list of services and training provided by the COR Audit Teams can be found in EKMS-1(series).

b. NCMS: If the ISIC, TYCOM, FLTCDR or CMS A&A Training Team is unavailable contact NCMS//N7//, the COR Audits and Training Department.

3. **CMS EDUCATION AND TRAINING**. In accordance with Article 455 to EKMS-1(series), the COMSEC Account Manager must develop, manage and ensure COMSEC training is part of the unit's long and short-range training schedule.

Training must be conducted at a minimum of monthly to ensure that all personnel handling COMSEC material are familiar with and adhere to proper COMSEC procedures. This training may be satisfied through required reading, stand-up presentation, or during the conduct of spot checks. The training must be documented to ensure it is verifiable during training visits or

COR Audits.

COMSEC Account Managers are also responsible for the proper training of remote LEs and for ensuring Commanding Officers/OICs of their remote LEs (Issuing) are conducting, documenting and submitting quarterly spot checks required by EKMS-1(series).

a. Formal Training. Each automated (EKMS or KMI) account must have a minimum of (2) properly cleared, formally trained Account Managers at all times. Formal training is available in all major fleet concentrated areas and areas where the Marine Corps Expeditionary Forces (MEFs) are located. Formal training must be completed prior to appointment of personnel. . Should operational requirements prevent compliance within 90 and 180 days respectively, a waiver for continued appointment must be requested in writing through the units' chain of command from NCMS

b. The KMI-Interactive Courseware (ICW) is a prerequisite for attendance in the formal KMI Manager COI and is available on the Total Workforce Management System (TWMS), the My Navy portal, the Navy Information Application Product Suite (NIAPS) server for afloat units and the Navy E-Learning (NEL) ashore and afloat. The course must be successfully completed every 3 years for active COMSEC Account Managers and COR Auditor personnel. Additional information including minimum hardware and software requirements can be found in Chapter 6 to EKMS-1(series) Supp-1.

c. Interim Qualification (Job Qualification Requirement (JQR) **EKMS Accounts Only**. When training cannot be completed prior to appointment due to quota non-availability, operational requirements, etc… personnel appointed to manage an EKMS account must complete the EKMS Manager (JQR) within 90 days of appointment. The JQR is available on the NCMS SIPRNet CAS portal. Presently, a JQR has not been developed for of KMI Account Managers.

d. Personnel Qualification Standards. All USN military personnel appointed or designated as; COMSEC Account Managers, Alternates, Clerks, or LE's must complete the applicable section of the latest version of NAVEDTRA 43462-1 (EKMS) or 43462-2(KMI) for the position occupied. At the discretion of the CO, civilian employees and contractor personnel whose duties require access to COMSEC material may be required to complete the applicable portions of the PQS. If required, this should be communicated in position descriptions, individual development plans and performance plans.

PQS is not intended to nor does it replace formal classroom training nor does completion of formal training negate the requirement to complete the PQS.

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

4. **COMSEC SERVICES**

a. COMSEC MATERIAL ISSUING OFFICE (CMIO). CMIO is located in Norfolk, VA and receives, stores, and ships Ready for Issue (RFI) equipment.

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. An original USTRANSCOM Form 10 with the CO's signature is maintained by DCS. With each delivery/pick-up from DCS, the COMSEC Account Manager must present an identical copy of the USTRANSCOM Form 10 with original signature to the DCS courier.

c. CMS COR AUDIT TEAMS. The CMS COR Audit Teams are located in all major fleet concentrated areas, as well as Okinawa, JA. COR Audit teams are chartered to provide training to CO's, SCMSRO's, COMSEC Account Managers and LE personnel. Each team is responsible for a specific geographical region as reflected in EKMS-1 (series). These teams should be viewed as "First Responders" for fleet assistance in COMSEC matters. It is **highly recommended** commands take advantage of the training and assistance available from the local COR Audit team.

The COR Audit Teams visit each DON COMSEC account approximately every 18 months and typically within 90 days of the next biennial COR Audit. These visits provide an independent review of account management to ensure compliance with Navy and National policy and afford an opportunity for improvements in account management. At the conclusion of the visit, an out-brief will be conducted with the CO to inform the command of the training conducted, areas where deficiencies or weaknesses were noted, including any COMSEC incidents or PDSs discovered and provide recommendations to mitigate or prevent reoccurrence. The findings and recommendations presented are privileged communications and will not be divulged outside of the command visited.

NLT 30 days following the training visit and every 30 days thereafter, as applicable, COMSEC Account Managers will submit a

written update on discrepancies documented during the visit to the CO of the account. Regardless of medium used to communicate the status, a copy of the status report(s) will be maintained at the unit in the accounts correspondence file with the associated visit report.

There are no fees or cost to the units visited for regularly scheduled visits. For on-site assistance or training outside the normal scheduled visits funded by NCMS, the requesting entity must request the assistance in accordance with Article 330 to EKMS-1(series).

d. COR AUDITS. NCMS//N7// manages the DON COR Audit Program. Auditors must be trained and certified by NCMS//N7//. All COMSEC accounts must undergo a COR Audit **every 24 months**. The audit will be conducted in accordance with the procedures contained in EKMS-3(series).

e. TOWN HALLS. Town Halls are hosted annually by NCMS when funding permits such and are primarily intended for COs, Account Managers, and COR Auditors. 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. Attendance at Town Halls is mandatory for Commanding Officers and COMSEC Account Managers however; it is highly recommended SCMSRO's and Alternates attend, when possible.

f. COMSEC INCIDENT TREND ANALYSIS MESSAGES. NCMS publishes an annual Trend Analysis ALCOM and related statistical data to illustrate areas in need of attention and improvement within the DON COMSEC community.

5. SELECTING A COMSEC ACCOUNT MANAGER.

a. The use of TAD personnel is not authorized and personnel appointed as COMSEC Account Managers, Alternates, Local Element Issuing or COMSEC Clerks must be permanently assigned to or employed by the command, as applicable.

b. The selection of personnel to serve as a COMSEC Account Manager and Alternate(s) should be made carefully and consider the sensitivity and criticality of the communications protected by the materials entrusted unto these individuals. Experience, not rank, should be the primary factor when selecting the Account Manager.

c. A COMSEC Account Manager should not be chosen solely on accounting or computer skills and should not be assigned on a short term basis; it takes several months to become familiar with proper day-to-day account management, related policies and use of the LMD/KP or MGC/AKP.

d. The COMSEC Account Manager is the principal advisor to the CO in all matters regarding COMSEC. It is essential the CO designate an individual who understands the unit's mission, COMSEC requirements and displays both sound judgment and decision making ability.

e. When personnel are selected through their orders, or for civilians, their position description (PD), a personal interview should be conducted to ascertain the individual's prior experience and qualifications. It is recommended individuals with no prior experience managing COMSEC material not be appointed as the Account Manager. It is recommended, if possible they be appointed as an Alternate Manager to become familiar with the duties and responsibilities under more an experienced and qualified individual.

f. A COMSEC Account Manager who is assigned too many duties, is insufficiently trained, demonstrates questionable decision making abilities and poor attention to detail can negatively impact mission readiness or jeopardize untold amounts of extremely sensitive information.

g. Each numbered account will have a COMSEC Account Manager and a minimum of one alternate appointed in writing by the current Commanding Officer. If the accounts Highest Classification Indicator (HCI) is TOP SECRET, it is highly recommended two additional alternates be appointed. This will ensure at least two personnel have the "A" or "B" combinations, as applicable to maintain Two Person Integrity (TPI) purposes during periods of leave, TAD, etc. Additional requirements for Account Management personnel:

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

(a) COMSEC Account Managers must meet the following minimum requirements: Commissioned Officer, E-6 or above (or selectee), GS-7 or above, all with a minimum of six months government or commissioned service not including duty under instruction or in training but may include six or more years of prior enlisted service for Commissioned Officers. Alternate

Account Managers must hold the minimum grade of E-5, GS-6 or Commissioned Officer.

> **Note:** Commanding Officers are authorized to waive the length of government service required for COMSEC Account Managers. Waivers of this requirement must be documented locally and retained by the account and the ISIC until no longer in effect. Do not submit copies of length of service waivers to NCMS.

(b) Contractor personnel are **not** permitted to serve as a COMSEC Account Manager or Alternate without a waiver from NCMS.

(2) COMSEC Account Managers and Alternates must possess a security clearance equal to or higher than the HCI of the account. For accounts with a HCI of TOP SECRET, the incumbents SSBI must be current within (5) years. If the account is validated for/holds keying material intended for use on SCI/SI circuits the Manager(s) must also be SCI eligible at the time of appointment. See Articles 412 and 425 to EKMS-1(series) regarding Temporary Access (interim clearances) and the limitations related to such.

(3) Personnel requiring access to COMSEC material must be authorized access in writing by the current CO or other official as "Acting" in the capacity of the CO. The use of "By Direction" is **not** authorized for Letters of Appointment or access lists used for granting access to restricted areas and to COMSEC.

(4) Personnel selected to be a COMSEC Account Manager or Alternate must successfully complete formal training **prior to appointment**. See Articles 412 to EKMS-1(series) for EKMS Accounts or Article 601 to EKMS-1(series) Supp-1 for KMI Accounts when operational requirements or quota limitations prevent attendance in formal training prior to appointment.

(5) There is no restriction on the length of time an individual may perform COMSEC Account Manager duties.

(6) During the temporary absence of the Manager, up to a maximum of 60 days, the Primary Alternate must administer the account. If the Manager is absent for more than 60 days, a new Manager must be appointed. The Commanding Officer of the account command may direct an account inventory be conducted prior to, during, or after the temporary absence of the Manager.

(7) The Position Description (PD) of civilian employees

must specify COMSEC Account Manager duties as a full-time position prior to appointment as a Manager or Primary Alternate.

SECTION III

1. **COMSEC INCIDENT REPORTING.**

a. The COMSEC system has been designed to provide a means for reporting deviations from prescribed policy and procedures and taking corrective action. These deviations may jeopardize or have the potential to jeopardize national security. Reports of any incident must be made irrespective of the judgment of the COMSEC Account 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.

b. Timely reporting of COMSEC incidents is paramount to mitigating the impact to operational readiness and is necessary for Controlling Authorities or Command Authorities to determine the appropriate actions to direct.

c. 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. 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 FT George G Meade or NCMS Washington DC by other secure means to provide information concerning the incident.

d. Reporting time frames are driven by the status and type of material involved however; all incidents must be reported NLT 72 hours from the time of discovery. See Article 960 to EKMS-1(series) for specific timeframe guidance.

2. **COMSEC INCIDENTS AND COMSEC INSECURITIES.** The distinction between these two terms is the former has yet to be investigated and evaluated whereas in the later, the matter reported has been investigated and evaluated.

a. A COMSEC incident is 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.

b. A COMSEC Insecurity is 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.

3. **TYPES OF COMSEC INCIDENTS.** There are (3) three types of COMSEC incident; Cryptographic, Personnel and Physical. A listing of COMSEC incidents can be found in Article 945 to EKMS-1(series) and Article 805 to EKMS-1(series) Supp-1. Additional device-specific incidents may be contained in the Operational Security Doctrine (OSD) for the device. OSDs can be found at: www.iad.nsa.smil.mil – IA Library – Doctrine.

4. **COMSEC INCIDENT EVALUATION.** COMSEC incidents are evaluated as:

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

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

5. **PRACTICES DANGEROUS TO SECURITY (PDS).** Although not reportable at the national level (NSA), if allowed to perpetuate, PDS's have the potential to jeopardize the security of COMSEC material.

There are (2) types of PDSs; Non-Reportable and Reportable. All PDS's must be documented and reported to the CO of the account (non-reportable PDS) or externally (reportable).

A listing of PDS's can be found in Chapter 10 to EKMS-1(series) and Chapter 9 to EKMS-1(series) Supp-1 for KMI accounts. All COMSEC accounts must conduct PDS familiarization training annually that will, at a minimum, include a review and discussion of Chapter 10 to EKMS-1(series) or Chapter 9 to EKMS-1(series) Supp-1.

SECTION IV

1. **COMSEC INVENTORIES**. Inventories are required at a minimum of semi-annually to ensure all COMSEC material is properly and continuously accounted for. Inventories are also required to be conducted to document a Change of Account Manager, Change of Command and upon disestablishment of an account.

2. **WHO CAN CONDUCT AN INVENTORY.** Inventories must be conducted by the COMSEC Account Manager and Alternate or one of the two and a properly cleared and authorized witness except as discussed below. To ensure the responsibility for accurate and proper completion of the inventory is maintained throughout, the two individuals who start the inventory should be the ones who complete it. Inventories conducted to document a Change of Account Manager or LE Issuing must be conducted by the outgoing person and witnessed by the incoming person.

Block 17 on the final page of inventories used to document a Change of Command, OIC, or SCMSRO must be signed by the outgoing CO/OIC or SCMSRO, as applicable. The incoming CO/OIC or SCMSRO may initial the report, if desired, but it is **not required**.

The physical inventory may have some items lined-out. Line-outs must be initialed by the two personnel conducting the inventory and are used to indicate material which has been destroyed or transferred after generation of the inventory report. The corresponding date of the report or applicable Transaction Number must be reflected in the Remarks Column and line-outs require supporting documentation be on file with the Manager. If accounting reports are submitted to the COR as required, line-outs should be few in nature.

If there are multiple line outs, it is recommended the accounts most recent monthly Pending Receipts report provided by NCMS and results of the most recent Change of Account Location (COAL) inventory be reviewed with the Manager.

With exception to submarines at-sea, all Account Managers are required to conduct a COAL inventory monthly. This is not a physical inventory but a tool which will present, for corrective action a list of accounting discrepancies in the form of an Inventory Reconciliation Status Transaction (IRST). The IRST reflect discrepancies which exist in the unit's local inventory and that reflected on file in Tier-1.

3. **LOCAL ELEMENT MATERIAL**. The Account Manager and Alternate

(or properly cleared and authorized witness) should physically sight inventory all material, unless the account supports LEs located outside the vicinity of the supporting account where such is not practical. In this scenario, the Account Manager can generate and provide an inventory to the LE and have the LE and a qualified witness conduct the inventory for material issued to them

4. **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, timely communication with the COR is essential.

5. **COMMON ACCOUNT DATA (CAD):** The CAD is the primary means used by the COR to determine Point Of Contact information for DON COMSEC Accounts. COMSEC Account Managers must review and update their CAD when a change in account management occurs and periodically thereafter to ensure the accuracy of the information contained. 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 Technical Support Center or other agencies due to incorrect contact information e.g. phone numbers, email addresses, etc.

Additional information related to inventories, CAD data, reconciliation and the inventory process can be found in Article 766 to EKMS-1(series).

SECTION V

1. **CMS SPOT CHECKS.** The CO is charged with the ultimate responsibility for the proper management and operation of their command's COMSEC Account. Top-down Chain of Command engagement in COMSEC matters is critical to the health of the account. It is both the CO's duty and responsibility to ensure that unannounced spot checks are conducted on the COMSEC Account (Vault) and LE Work Centers where COMSEC material is handled, used and stored.

When conducted, unannounced spot checks heighten awareness and attention to detail, improve the security posture of the unit and enhance the accountability and safeguarding of highly sensitive materials. Spot checks also provide the ability to identify deficiencies and implement corrective measures prior to the account biennial COR Audit.

2. The CO, OIC or SCMSRO, as applicable is required to conduct a minimum of (1) spot check per quarter and may delegate **no more than two** of the four quarterly spot checks to the Executive Officer. SCMSROs may delegate two of the four spot checks to the Communications Officer (COMMO) if the COMMO is not designated as the Account Manager or Alternate.

3. COMSEC Account Managers and Alternates are required to conduct a minimum of (1) one spot check per calendar month on supported local elements and a semi-annual self-assessment using EKMS-3(series). When conducted objectively, there should not be significant disparities between the results of a unit-conducted semi-annual self-assessment and the COR Audit.

4. For external LE's, the CO, OIC or SCMSRO, as applicable, will ensure spot checks are conducted, retained on file by the respective Work Center and a copy is submitted to the supporting COMSEC Account Manager.

5. **CO SPOT CHECK GUIDE.** The guide contained herein consists of (2) tabs; Tab A is for use in conducting Spot Checks at the account level; Tab B is for use in conducting Spot Checks at the Local Element (LE) level. The Spot Checks contained herein are tailored to individual areas and have been extracted from EKMS-3(series) which is used during COR Audits.

Commanding Officers and Executive Officers are encouraged to randomly select different Spot Checks for each quarter to gain a greater perspective on account management, where deficiencies may

exist and the level of engagement of the Manager and Alternates.

COMSEC Account 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 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. 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 in use, as required?

(4) Is there a SF-702 (Open/Closure Log) for security containers in use? (two are required for TPI containers)

(5) Is it being used properly (opened by/closed by/checked by)

f. Have the Manager show when the last changeover was conducted.

g. Ask the Manager to see the accounts Audit Trail Review log.

h. Ask the Manager for the most recent Change of Account Location (COAL) inventory and the Inventory Reconciliation Status Transaction. Are there discrepancies? If so, is the Manager actively working with a COR Manager at NCMS to resolve the discrepancies?

2. **SPOT CHECK SHEETS**. There are (2) tabs contained herein with spot checks for use at the Account or Local Element (LE) level. Spot checks for use at the Account level are contained in Tab A; those intended for use at the LE (workcenter) level are contained in Tab B.

TAB A SECTION 1 – SECURITY

Answer	Area/Item Reviewed
Yes / No	1. Are adequate visitor controls enforced to ensure access to classified information is given only to visitors who possess the proper identification, security clearance, and Need to Know? [SECNAV-M 5510.30 (Series), Article 11-1 paragraph 2, 3; SECNAV-M 5510.36, Article 7-12; EKMS-1 (Series), Article 550.e]
Yes / No	2. Is a visitor's register in use, properly maintained (all blocks filled out) and retained for one year? [EKMS-1 (Series), Article 550.e, Annex M]
Yes / No	3. Are the names of individuals with regular duty assignments in the COMSEC facility on a formal access list signed by the current CO/OIC/SCMSRO? [EKMS-1 (Series), Article 505.d, 550.e]
Yes / No	PART A: Are personnel whose duties require access to cryptographic information formally authorized in writing by the CO/OIC/SCMSRO? [EKMS-1 (Series), Article 505.d] PART B: If personnel are authorized access to COMSEC material on an access list, has the list been updated annually, upon change of command or whenever the status of an individual changes? [EKMS-1 (Series), Article 505.d]
Yes / No	4. Are security clearances for personnel who require access to classified COMSEC material equal to or higher than the material the member has access to? [EKMS-1 (Series) Articles 505, 945.e]
Yes / No	5. If the account is validated for/ holds keying material for SCI/SI circuits, are the Manager and Alternates SCI eligible? [EKMS-1 (Series), Article 412.d]
Yes / No	6. 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]
Yes / No	7. Is the exterior of each COMSEC security container free of markings which reveal the classification or description of the material stored therein? [SECNAV-M 5510.36, Article 10-1, paragraph 3]
Yes / No	8. Is the space/compartment or vault which contains COMSEC material outwardly identified as a "Restricted Area"? [OPNAVINST 5530.14(Series), Articles 210.g, 218.a; MCO 5530.14(Series) Article 3004]
Yes/No/NA	9. **For USMC accounts only**. Does the "Restricted Area" sign meet the criteria set forth in MCO 5530.14? [MCO 5530.14 (Series), Article 3004]
Yes / No	10. Are applicable security controls (guards and alarms) in place per SECNAV-M 5510.36, Chapter 10? [EKMS-1 (Series), Article 520.a]

Yes/No/NA	11. **For USMC accounts only.** Does the COMSEC office have an Intrusion Detection System (IDS) installed and is it checked at defined intervals? [MCO 5530.14 (Series), Article 3003]
Yes / No	12. Do storage containers meet the minimum security requirements for the highest classification of material stored therein? [EKMS-1 (Series), Article 520.d; SECNAV-M 5510.36, Chapter 10]
Yes / No	13. Is an Optional Form (OF-89) maintained for each security container; used to record damages; repairs or alternations and retained within the container? EKMS-1 (Series) Article 520.b; SECNAV-M5510.36 Article 10-15]
Yes / No	14. Is a Security Container Information Form (SF 700) maintained for each lock combination and placed in each COMSEC security container? [SECNAV-M5510.36, Article 10-12, paragraph 3; EKMS-1 (Series), Article 520.b]
Yes / No	15. Is a Security Container Check Sheet (SF-702) maintained for each lock combination of a COMSEC storage container? [SECNAV-M5510.36, Article 7-10; EKMS-1 (Series), Article 520.b]
Yes / No	16. Are completed SF-702s retained for 30 days beyond the last date recorded [EKMS-1 (Series] Article 520.b; SECNAV-M5510.36 Article 7-11
Yes / No	17. Except in an emergency, are combinations to the COMSEC vault/ facility/security containers restricted to the EKMS Manager and alternates only? [EKMS-1 (Series), Article 515.c]
Yes / No	18. If the COMSEC facility is **continuously** manned, are security checks conducted at least once every 24 hours and documented on a SF-701? [EKMS-1 (Series), Article 550.d]
Yes / No	19. In a **non-continuously** manned COMSEC facility, are security checks conducted prior to departure of the last person and documented on an Activity Security Checklist (SF-701)? [EKMS-1 (Series), Art. 550.d; SECNAV-M5510.36, Art. 7-11]
Yes / No	20. Are completed SF-701s retained for 30 days beyond the last date recorded [EKMS-1 (Series) Annex M; SECNAV-M5510.36, Article 7.11]
Yes / No	21. 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 and documented on a SF-701 to ensure that all doors are locked and that there have been no attempts at forceful entry? [EKMS-1 (Series), Article 550.d]
Yes / No	22. Does any one person have knowledge of both combinations to any one TPI container? EKMS-1 (Series), Articles 515.c, 945.e]
Yes / No	23. Are sealed records of combinations to COMSEC containers maintained in an approved security container (other than the container where the COMSEC material is stored), and available to duty personnel for emergency use? [EKMS-1 (Series), Article 515.e; 945.e]

Yes / No	24. Are combinations to COMSEC containers changed when initially placed in use, taken out of service, at least biennially, upon transfer/reassignment of personnel who have access, or when compromised? [EKMS-1 (Series), Article 515.b]
Yes / No	25. Are SF-700s protected as follows: [EKMS-1 (Series), Article 515.f]
	a. Individually wrapped in aluminum foil and protectively packaged in an SF-700 envelope?
Yes / No	b. Are SF-700s sealed using transparent lamination or plastic tape?
Yes / No	c. Are names, addresses and phone numbers of individuals authorized access to the combination clearly recorded on the front of the envelope?
Yes / No	d. Proper classification and downgrading markings on Part 2 and 2A
Yes / No	e. Are the envelopes inspected monthly to ensure they have not been tampered with and the COR Audit findings documented on a locally generated log?
Yes / No	26. 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]
Yes / No	27. Are software-designed devices in storage at the account level covered as part of the unit's 3M or other service-specific maintenance program? [EKMS-5(Series), Article 313]
Yes / No	28. Is COMSEC material properly stored when not in use or under the direct control of authorized personnel? [EKMS-1 (Series), Article 520.a]
Yes / No	29. Are COMSEC files, records and logs handled and stored in accordance with their overall classification? [EKMS-1 (Series), Article 715.a; SECNAV-M 5510.36, Article 6-3, 6-26]
Yes / No	30. Do classified COMSEC files, records and logs reflect proper classification markings, the derivative source for the classification and declass/downgrading instructions? [EKMS-1 (Series), Article 715.d]
Yes / No	31. Are in-use In-Line Network Encryptors (INEs) such as KG-175s, KG-250s, or KIV-7Ms compliant with NSA directed mandatory software upgrades and if not, has DIRNSA or NCF issued and official waiver, in writing? [EKMS-1 (Series) Article 945.c]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 2 – ACCOUNT MANAGER RESPONSIBILITIES

Answer	Area/Item Reviewed
Yes / No	01. Has a formal Letter of Appointment (LOA) been completed for the Manager, Alternate(s) and Clerk(s) and signed by the current CO/OIC? [EKMS-1 (Series), Articles 412, 414 and Annex F; EKMS-1 Supp-1, Article 407.b]
Yes / No	02. Are SD 572 forms: [EKMS 1(Series) Articles 410, 769.b and Annex M; [EKMS-1(series) SUPP-1, Articles 409.a, 705.a, Figure 4.4] a. Executed and on file for all personnel with access to "S" or "TS" cryptographic information, including Account Managers? b. Retained for 90 days after the individual no longer requires access to COMSEC material, transfers or retires?
Yes / No	03. **EKMS Accounts only:** Has the Manager and Alternate successfully completed formal training prior to appointment or completed the EKMS Manager Job Qualification Requirement within the prescribed timeframe (JQR)? [EKMS-1 (Series) Article 412.f]
Yes / No	04. Is the EKMS or KOAM Manager Turnover Checklist used utilized during Account turnovers and retained as required M? [EKMS-1 (Series), Articles 766.a, 455; Annexes M, R]
Yes/No/NA	05. If formal training for Manager or Alternates was not completed prior to appointment due to extenuating circumstances, has the Service Authority granted an official waiver in writing for the appointment? [EKMS-1(Series) Supp-1, Article 601.b]
Yes/No/NA	06. **KMI Accounts only:** Has the TSO completed the NSA developed Computer-Based Training in the required timeframe? [EKMS-1(Series) Supp-1, Art 411.c; Figure 6-1]
Yes/No/NA	07. **KMI Accounts only:** Has the CPA and a CPSO been appointed in writing? [EKMS-1(SERIES) Supp-1, Articles 403.a, 405, 407, 411.i Figure 4-6, 411.e, 411.i] **Note:** A separate appointment letter is not required for the KOAM or Alternate if the incumbent is also fulfilling the role of the Client Platform Administrator (CPA).
Yes/No/NA	08. **KMI Accounts only:** Does the CPA have a minimum SECRET security clearance? [EKMS-1(Series) Supp-1, Articles 411.e, 805.c; DOC 042-12]
Yes/No/NA	09. **KMI Accounts only:** Is the KOAM, CPSO and CPA trained and certified per the incumbent's cybersecurity category or specialty area code? [EKMS-1(Series) Supp-1, Articles 411.e, 411.i, 609.a, 903.a; DOC 042-12; SECNAV M5239.2]
Yes/No/NA	10. **KMI Accounts only:** Has both the CPA and CPSO completed the NSA-developed CBT? [EKMS-1(Series) Supp-1, Articles 411.e, 411.i, Figure 6-1; DOC 042-12]
Yes/No/NA	11. **KMI Accounts only:** Have both the CPA and CPSO executed the required Information System Privileged Access Agreement? [EKMS-1(Series) Supp-1, Articles 403.a, 411.e, 411.i; Annex I]

Yes/No/NA	12. **KMI Accounts only:** Does the CPSO have a minimum security clearance equal to or higher than the HCI of the account? [EKMS-1(Series) Supp-1, Articles 411.i, 805.c; DOC 042-12]
Yes/No/NA	13. **KMI Accounts only:** Does the PLT1RA conduct annual face-to-face verification for each active "Human User"; is the date and time of the reverification documented locally? [EKMS-1(Series) Supp-1 Articles 345.c, 501.b; DOC 043-12]
Yes / No	14. **KMI Accounts only:** Has the each Account Manager completed the DON Basic COMSEC Policy & Procedures Inter-Active Courseware (ICW) as required? [EKMS-1(Series) Supp-1 Ch. 6]
Yes / No	15. Has the Manager promulgated written guidance, concerning the proper handling, accountability, and disposition of COMSEC material? [EKMS-1 (Series), Article 455.e, Figure 4-4]
Yes / No	16. Are self-assessments and spot checks conducted by the Manager or Alternates and retained locally as required? [EKMS-1 (Series) Articles 315.b, 450.i, 455.y, 1005.a; Annex M paragraph 2]
Yes / No	17. If contractor personnel are assigned to and have access to COMSEC material at a DON activity, does the 254 and does Block 10 indicate the access is required? [EKMS-1 (Series) Article 505.g]
Yes / No	18. Prior to releasing COMSEC material to a contractor account, has the Manager ensured the provisions of OPNAVINST 2221.5 (Series) have been met? [EKMS-1 (Series), Article 505.g]
Yes / No	19. If the account has LEs responsible to a CO other than the CO of the account, have Letters of Agreement been exchanged and signed? [EKMS-1 (Series), Article 445.a; Annex G]
Yes / No	20. Does the Letter/Memorandum of Agreement address the minimum areas in accordance with [EKMS-1 (Series) Annex G?]
Yes / No	21. Has coordination been made with the area Defense Courier Service (DCS) station to establish a DCS account by submission of a USTC Form 10 signed by the current CO/OIC/SCMSRO? [EKMS-1 (Series), Articles 405.h, 751.b; EKMS-1(Series) Supp-1 Articles 403.a, 705.a.1]
Yes/No/NA	22. Does the Manager ensure personnel who perform cryptographic maintenance in the organization have a DD-1435 documented on file and are authorized in writing by the Commanding Officer to perform cryptographic maintenance? [EKMS-1 (Series), Article 945.e, EKMS-5 (Series), Article 111]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 3 - LMD/KP MGC/AKP

Answer	Area/Item Reviewed
Yes/No	01. Is unescorted access to the area where the LMD/MGC is located restricted to cleared personnel authorized access to the space or account Managers?? [EKMS-1(Series, Article 505.d; Annex Q, Paragraph 1 and 8; EKMS-1(Series) Supp-1 Article 209.c]
Yes / No	02. Are passwords for each account, including the "CPA" or "root" account on the MGC/LMD, as applicable changed every 90 days? [EKMS-1(Series) Supp-1 Article 215.a; EKMS-1(Series) Article 515.i, Annex Q Para 12; DOC-032-12] **Note**: On the LMD try to logon with the default generic root password. If unsuccessful, have the Manager logon as root, left-click on the mouse, go to – Desktop, - select Account Manager, select the target user "root", from the top, select "Users" – Password Restrictions – Expiration and review the "Last Successful Change" entry. On the MGC, look in the Windows Event Viewer for the account and event ID: 4738. This can also be verified on the individual SF-700 protecting the password.
Yes / No	03. Is the LMD/MGC configured to lock out an account after 3 failed logon attempts? [EKMS-1(SERIES) Supp-1 Article 215.a; EKMS-1(Series) Article 515.i]
Yes / No	04. Are all PINs/Passwords for accounts registered on the LMD/KP or MGC/AKP recorded and sealed in separate SF-700 envelopes for each user and protected as required? [EKMS-1 (Series), Articles 515.f, 520.j, 945.e; EKMS 1B Supp-1, Article 215.a]
Yes / No	05. Has the Manager ensured the account's CAD data is current and updated, as required? [EKMS-1 (Series) Article 455 and 602; EKMS-1(SERIES) Supp-1 (Series) Article 309.c]
Yes / No	06. Has the account performed an AKP/KP rekey at a minimum of annually? [EKMS-1(SERIES) Supp-1 (Series), Article 207.c, EKMS-1 (Series) 1005.a, Annex Q, paragraph 12] **On the LMD**: Follow the procedure above, change the alpha to KP Rekey and the start date to 366 days earlier, i.e. if the COR Audit is conducted on 02 Feb 13, use 20120201 as the date. Any rekey performed in the last year will appear in the window. If not from the **LCMS menu, select KP->Rekey KP Vectors->Request KP Rekey and verify the Firefly vector set has not expired. On the MGC: Navigate to MGC Management – AKP Configuration - AKP Vectors.**

Yes / No	07. Has the AKP, KP or KOK-23 been returned to CMIO or the depot, as applicable for recertification within 30 days of receipt of the replacement unit? [EKMS-5 (Series) Article 202]
Yes/No/NA	08. If the account has a KOK-23, has the device been certified within the current (3) years? [DOC 027-09 paragraphs 22 and 27; EKMS-1 (Series) Articles 945.c, 1005.b]
Yes/No/NA	09. If a KOK-23 is held, are the SSO and Operator CIK(s) accounted for in LCMS or the MGC, as applicable as ALC-1 and ALC-4, respectively? [DOC 027-09 paragraph 7.b; EKMS-1 (Series) Article 945.e]
Yes/No/NA	10. Has the account generated, wrapped and submitted a COAL inventory on a monthly basis? [EKMS (Series) Article 766.b; EKMS-1(SERIES) Supp-1, Figure 7-4] **Note:** N/A for submarines at-sea. **To verify in LCMS:** 1. From the desktop 2. Accounting 3. Transaction 4. Display (Adjust to originated between and use a two month Window; example 20100201 (beginning) 20100228 (ending) 5. Look for a transaction type of "inventory" 6. Verify it is "processed" 7. Select the inventory and view the transaction to determine if the type is "Change of Account Location" **To verify in MGC:** 1. Products – Reports – Transaction Status Log. 2. In the filter block under the In/Out box, type "inventory" to retrieve every inventory and IRST. 3. Report Date Down Arrow – Sort Descending or Ascending – **Ask the KOAM if COALs are performed at the beginning or end of month.** 4. Highlight an entry, look under "Related Log ID" column to find Log # 5. Look under the "Log ID" column to find the Log ID number which will be the IRST for that Inventory. 6. If there is no Log Number under the "Related Log ID" Column, look under the "Transaction Status" column, if the status is sent, the KOAM did not download the "IRST and Reconcile"
Yes/No/NA	11. Does each Manager have a (unique) LMD/KP Operator ID and CIK? [EKMS-1 (Series), Annex Q, Paragraph 12]
Yes/No/NA	12. Are REINIT 1 and NAVREINIT 2 keys classified at the level of the account's HCI and safeguarded appropriately? [EKMS-1 (Series), Article 1140]

Yes/No/NA	13. Are REINIT 1 and NAVREINIT 2 CIKS properly registered in LCMS? [EKMS-1 (Series), Article 1140] 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? b. Are NAVREINIT 2 keys reflected on the AIS as "Equipment" and accounted for as ALC-4?
Yes/No/NA	14. Does the account have a minimum of two LCMS/KP System Administrators registered? [EKMS-1 (Series), Annex Q, Paragraph 9]
Yes/No/NA	15. Are KP PINs changed every 90 days? [EKMS-1 (Series) Article 520.i, 1005.a]
Yes/No/NA	16. Has a KP changeover been performed every 3 months (92 days maximum)? [EKMS-1 (Series), Article 238.b, 945.c, Annex Q, paragraph 12] To determine, have the Manager or Alternate 1. Logon to LCMS. 2. Select "Maintenance". 3. Request KP Changeover
Yes/No/NA	17. Has the KP in use been recertified within the current (3) years? [EKMS-1 (Series), Article 945.c, Chapter 11]
Yes/No/NA	18. Is backup media labeled as "Secret", reflects proper downgrading instructions and the date the backup was performed? [EKMS-1 (Series), Article 718.c Note 2; EKMS-1(Series) Supp-1, Figure 2-2; SECNAV M5510.36]
Yes/No/NA	19. Is LCMS accounting data archived on a semi-annual basis after each fixed cycle inventory? [EKMS-1 (Series) Article, 1005.a, Annex Q, paragraph 12]
Yes/No/NA	20. Is archived media properly labeled, safeguarded and retained for four years as required? [EKMS-1 (Series), Article 1005.a, Annex M, Annex Q, paragraph 12]
Yes/No/NA	21. Are backups being performed on the following as required? [EKMS-1(Series), Articles 718.d, 1005.a]
Yes/No/NA	a. LCMS Database: After every session that modifies the Account Item Summary and Transaction Status log?
Yes/No/NA	b. Unix maintenance backups on monthly basis (i.e. Root and U)?
Yes/No/NA	22. Does the account maintain a KP CIK and PIN log; is the log being retained for the prescribed time frame? [EKMS-1 (Series), Article 1005.a]
Yes/No/NA	23. Does each account have two (2) AKP operationally affiliated CIKs (One primary; one backup)? [EKMS-1(Series) Supp-1, Articles 207.a, 903.a]
Yes/No/NA	24. Has a changeover been performed at a minimum of every 12 months? [EKMS-1(Series) Supp-1 Articles 207.d, 805.a]

Yes/No/NA	25. Are monthly visual COR Audits for the AKP conducted and documented properly in the AKP COR Audit Log? [EKMS-1(Series) Supp-1, Articles 201.d, 903.a]
Yes/No/NA	26. Has the KOAM conducted a rekey of the AKP and Type-1 Token (KOV-29) IA(I) and IA(M) certificates annually or as soon thereafter when operations permit? [EKMS 1B Supp-1, Articles 205.e, 903.b]
Yes/No/NA	27. Has the AKP in use been recertified within current (7) years? [EKMS 1B Supp-1, Articles 207.g, 805.a]
Yes/No/NA	28. Are AKPREINIT flash drives protected under TPI (dual combination lock) or with NSA-approved tamper-evident bags? [EKMS-1(Series) Supp-1, Articles 209.b, 805.c]
Yes/No/NA	29. If the account's HCI is "S" and tamper-evident bags are used in lieu of TPI, are the tamper-evident bags inspected: (1) daily or upon next opening of the container by a KOAM or Alternate and (2) jointly by both monthly? [EKMS-1(Series) Supp-1, Articles 209.b, 903.a]
Yes/No/NA	30. Does the account maintain two sets of AKPREINIT 1 and 2 drives and are they accounted for and reflected on the Product Inventory as "ALC-2", "equipment"? [EKMS-1(Series) Supp-1 Articles 209.b, 903.a; Figure 2-1]
Yes/No/NA	31. Are the AKPREINIT flash drives tagged and labeled to indicate the Short Title, Version Number and Account Number? [EKMS-1(Series) Supp-1 Article 209.b]
Yes/No/NA	32. Are the AKP USB Drives labeled SECRET, ALC 2, and accounted for as Short Title "KOM 3", "Equipment" in the Product Inventory? [EKMS-1(Series) Supp-1 Figure 2-1]
Yes/No/NA	33. Has an exact copy of archived accounting data been sent to the Central Service Node (CSN) within 30 days of the archive? [EKMS-1(Series) Supp-1, Articles 501.a, 903.a]
Yes/No/NA	34. Are backup media labeled as "Secret", reflect proper downgrading instructions and the date the backup was performed? [EKMS-1 (Series), Article 718.c Note 2; EKMS-1(Series) Supp-1, Figure 2-2; SECNAV M5510.36]
Yes/No/NA	35. Are backups of the MGC database performed after; every session that modifies the Product Inventory and Transaction Status log, a minimum of weekly and upon completion of a changeover? [EKMS-1(Series) Supp-1 Articles 207.d, 501.a, 903.a]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 4 - CHRONOLOGICAL FILE/ACCOUNTABLE ITEM SUMMARY (AIS)/TRANSFERS & RECEIPTS/LOCAL CUSTODY

Answer	Area/Item Reviewed
	01. Does the CHRONOLOGICAL FILE contain the following: [EKMS-1 (Series) Article 703.a, Annex M]
Yes/No/NA	a. COMSEC material accounting reports (conversion, destruction, generation, possession, receipts, relief from accountability, transfer reports).
Yes/No/NA	b. **EKMS Accounts only:** Up-to-date Accountable Item Summary (AIS) or up-to-date printed COAL inventory
Yes/No/NA	c. **KOA only:** Up to date printed Product Inventory or a Free Form text version of the Inventory Reconciliation /COAL inventory (EKMS-1(SERIES) Supp-1, Figure 7-4]
Yes/No/NA	d. Consolidated inventory reports (including ALC 4 & 7 inventories) and reconciliation notices
Yes/No/NA	e. Transaction Status Log
Yes/No/NA	f. USTRANSCOM Form-10
Yes/No/NA	g. CMS Form 1 (if required)
Yes/No/NA	h. SD Form 572
Yes/No/NA	i. EKMS CF Special Notices
Yes/No/NA	j. KMI Form 004 – KMI Human User Agreement Form [EKMS-1(SERIES) SUPP-1 Article 321.d, 409.a]
Yes/No/NA	k. KMI Form 005 – KMI Transition Checklist [EKMS-1(SERIES) SUPP-1 Article 401.b]
Yes/No/NA	02. Does the AIS or Product Inventory reflect all COMSEC-accountable material held by the account? [EKMS-1 (Series) Articles 763.a, 945.e, 1015; EKMS-1(SERIES) Supp-1, Articles 701.c, 805, 903]
Yes/No/NA	03. Are non-COMSEC accountable items such as SKL CIKS, CHVP products, etc. accounted for in LCMS or the MGC? [EKMS-1 (Series), Articles 706.a, 1005.a; EKMS-1(SERIES) Supp-1 Articles 701.c, 903.a]
Yes/No/NA	04. Is the Transaction Status Log closed out annually and maintained on file for (2) years? [EKMS-1(series) Article 724; Annex M; EKMS-1(SERIES) Supp-1, Articles 701, 703]
Yes/No/NA	05. Are hard copy SF-153s for physical material properly completed and reflect the: TN number, date assigned, and type of action, Manager and witness signatures? [EKMS-1 (Series) Article 1005.a.1, Annex N, paragraph 9]
Yes/No/NA	06. Have Destruction, Generation, Possession, Relief from Accountability and Transfer reports for ALC-1, 2 and 6 materials been sent to Tier 1 or the PRSN via x.400 as applicable? [EKMS-1 (Series) Article 730; EKMS-1(SERIES) Supp-1, Article 701.h]
Yes/No/NA	07. Are receipts for physical material, Bulk Encrypted Transactions (BETs) or report of corrupt BETs submitted within 3 business days of receipt or download to the COR or originator via X.400 or PRSN? [EKMS-1 (Series) Article 742, 1005.a; EKMS-1(SERIES) Supp-1, Article 705.a]

Yes/No/NA	08. Has the receipt of Two Person Control (TPC) material been reported per CJCSI 3260.01? [EKMS-1 (Series), Article 255.c]
Yes/No/NA	09. Are pending tracers processed within the required timeframes? [EKMS-1 (Series), Articles 743.e, 945.e]
Yes / No	10. Does the local custody file contain signed, effective, local custody documents for each item of COMSEC material issued *including electronic key issued to a DTD, SKL or TKL*? [EKMS-1 (Series), Articles 712.a, 945.e; Annex M, Annex T paragraph 17, Tab 1 paragraph 3]
Yes / No	11. Are local custody documents retained for a **minimum** of 90 days from the date the material is returned to the manager, destroyed or reflected on the next LE conducted inventory? [EKMS-1 (Series), Article 945.e.6, Annex M, paragraph 2]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 5 - DESTRUCTION PROCEDURES/REPORTS

Answer	Area/Item Reviewed
Yes/No/NA	01. Is routine destruction of physical COMSEC material performed using approved methods? [EKMS-1 (Series), Articles 540.j, 790.e and 945.e?]
Yes/No/NA	02. Are destruction records completed to document destruction of all COMSEC material? [EKMS-1 (Series), Article 736.b, Annex M]
Yes/No/NA	03. Is destruction of key issued to a SKL/TKL or other electronic storage device completed and verified? [EKMS-1 (Series), Article 540.c; 945.e, 1005.a; DOC 005-15; 024-12]
Yes/No/NA	04. Do destruction records clearly identify the short title, edition(s), accounting number, ALC, date of destruction, the printed name and signatures of the persons who performed and witnessed the destruction and are blocks 14 & 16 annotated to indicate the action the SF-153 was used for (destroyed/witness?[EKMS-1 Series), Article 736.a; Article 790.f; and Figures 7-1-3 paragraph 4, 7-2-2 paragraph 2, 7-3-1 paragraph 2, Annex N]
Yes/No/NA	05. Is superseded COMSEC material or equipment authorized for destruction destroyed within the proper timeframes? [EKMS-1 (Series), Articles 540.e, 540.h, 945.e, 1005.a]
Yes/No/NA	06. - Have the following items been recorded as "Destroyed" or "Filled in End Equipment" NLT the 5th day of the month following use/loading? [EKMS-1 (Series), Articles 238, 540, 1005.A, 1140; Annex Q para 10; EKMS-1(SERIES) Supp-1, Articles 207.b, 207.c, 903] - FF Vector Set: USFAU 0000000333 - Message Signature Key: USFAU 4294967297 - Transit CIK: USKAU B7121 [EKMS Account only] - KG Rules: USKAD BU71260 880091 [EKMS Account only] - KG-250 key AFAU 1401600001 [KMI Account only]
Yes/No/NA	07. Have consolidated destruction records been signed by the CO/OIC/SCMSRO (Block 17)? [EKMS-1 (Series), Annex N, paragraph 7.a]
Yes/No/NA	08. Are SAS/TPC destruction reports signed by two members of the SAS/TPC Team? [EKMS-1 (Series), Annex N, paragraph 7.b]
Yes/No/NA	09. **For afloat units in port without an NSA-Evaluated/Authorized Destruction Device.** Is non-paper COMSEC material being destroyed with a cross-cut shredder and the residue temporarily retained until it can be disbursed at sea? [EKMS-1 (Series), Article 540.j, 945.e]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 6 – INVENTORY REPORTS & CORRESPONDENCE, MESSAGE AND DIRECTIVES FILE

Answer	Area/Item Reviewed
Yes / No	01. Is all COMSEC material (including equipment and publications) assigned AL Code 1, 2, 4, 6, and 7 inventoried semiannually? [EKMS-1 (Series) Article 766.a; Annex N] **Note:** Operational SSBNs and SSGNs are exempt from fixed-cycle inventory requirements. During extended maintenance availability periods they will adhere to their normal FC Inventory cycle in accordance with Article 766.b.
Yes / No	02. Was the SAIR signed by the Manager, a properly cleared witness, and the Commanding Officer or SCMSRO? [EKMS-1 (Series), Annex N, Paragraph 7.a]
Yes / No	03. Is the completion of SAIR and CCIR inventories reported to the COR, as required? [EKMS-1 (Series), Articles 766.b; EKMS-1(SERIES) Supp-1, Article 707; Figure 7-4] **Note:** N/A for Change of Command inventories
Yes / No	04. Are "Request for Inventory Transactions" generated by the COR, responded to within 30 days of the initial request of the inventory? (EKMS-1 (Series), Article 766.b; Annex Z] **Note:** Submarines deployed or on patrol will use a locally generated inventory
Yes / No	05. Have discrepancies on the Inventory Reconciliation Status Report (IRST) been communicated to the COR and resolved? [EKMS-1 (Series), Article 766.b]
Yes / No	06. Was the CCIR or Combined Inventory, as applicable conducted for a change of command signed by the outgoing Commanding Officer? [EKMS-1 (Series), Articles 766.a, 766.b]
	07. Does the Correspondence and Message File contain the following required files: [EKMS-1 (Series), Article 709.a]
Yes / No	a. Account establishment correspondence?
Yes / No	b. Manager, Alternates and Clerk appointment correspondence (EKMS or KOAMs)?
Yes / No	c. **KOA only** - CPA and CPSO appointment correspondence?
Yes / No	d. **KOA only** - A signed copy of Information System Privileged Access Agreement and Acknowledgement of Responsibilities form. [EKMS-1(SERIES) Supp-1, Articles 411.e, 411.i; Annex I]
Yes / No	e. COMSEC Incident and Practice Dangerous to Security reports (this includes documentation on non-reportable PDSs)?
Yes / No	f. Correspondence relating to command allowance and authorization to store classified COMSEC material?
Yes / No	g. The previous CMS COR Audit report
Yes / No	h. List of personnel authorized access to keying material and the LMD/KP or MGC/AKP, as applicable?

Yes / No	08. Does the directives file contain a copy of each effective directive of the command and higher authority, which relates to COMSEC matters (e.g., guidance for LEs, Letters of Agreement (LOA), and waivers of COMSEC policy and procedures)? [EKMS-1 (Series), Article 709.c]
Yes / No	09. Does the Message File contain all effective general messages (i.e., ALCOMs, ALCOMPAC P, and ALCOMLANT A) that pertain to account holdings or COMSEC policy and procedures? [EKMS-1 (Series), Article 709.b]
Yes / No	10. Does the Manager maintain and provide up-to-date status information to LE personnel when promulgated by the various Controlling Authorities for material held by the account or issued i.e. JCMO 2116XXXXZ, COGARD C4ITSC, etc.? [EKMS-1 (Series), Art 255.f, Article 760.a]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 7 - COMSEC LIBRARY

Answer	Area/Item Reviewed
	01. Does the account maintain a COMSEC library with all applicable instructions and manuals? [EKMS-1 (Series), Article 721, EKMS-1(SERIES) Supp-1 Annex C]
Yes/No/NA	a. **EKMS Accounts only:** LMD/KP Operators Manual EKMS 704(series)
Yes/No/NA	b. **KOA Only:** Operations and Maintenance Manual (OMM) for the KMI Client Node (classified)
Yes/No/NA	c. **EKMS Accounts only:** EKMS Managers JQR
Yes/No/NA	d. COMUSFLTFORCOM/COMPACFLT/COMUSNAVEURISNT C2282.1 (series) Basic Shipboard Allowance of COMSEC material (USN Surface Ships only)
Yes/No/NA	e. EKMS-1 (series) Policy and Procedures Manual
Yes/No/NA	f. EKMS-3 (series) EKMS/KOA COR Audit Manual
Yes/No/NA	g. EKMS-5 (series) EKMS Cryptographic Equipment Manual
Yes/No/NA	h. COMDTINST 5510.23 (USCG only)
Yes/No/NA	i. NAG-53 (series) – Keying Standard for Non-Tactical KG-84/KIV-7 Point to Point Circuits (a**shore accounts only**)
Yes/No/NA	j. NAG 16 (series) Field Generation and Over-the-air distribution of tactical Electronic Key
Yes/No/NA	k. NSA Mandatory Modification Verification Guide (MMVG)
Yes/No/NA	l. OPNAVINST 2221.5 (series) Release of COMSEC material to U.S. Industrial Firms Under contract to USN
Yes/No/NA	m. SECNAV M5510.30 (series) DON Personnel Security Program
Yes/No/NA	n. SECNAV M5510.36 (series) DON Information Security Program
Yes/No/NA	o. OPNAVINST 5530.14 (series) Physical Security and Loss Prevention
Yes/No/NA	p. SECNAVINST 5040.3 (series) Naval Command COR Audit Program (if applicable)
Yes/No/NA	q. OPNAVINST 2221.3 (series) Qualifications of Maintenance Personnel
Yes/No/NA	r. CJCSI 3260.01 (series) Joint Policy Governing Positive Control Material Devices (**Required only if SAS material held**)
Yes/No/NA	s. SDIP 293 NATO Cryptographic Instruction (**Required only if account holds NATO material**)
Yes/No/NA	t. AMSG-600 NATO Communications Security Information. (**Required only if the account holds NATO material**)
Yes/No/NA	u. Operational Security Doctrine for Key Management Infrastructure (KMI) KOV-29 (sKey6500)
Yes/No/NA	v. Operational Security Doctrine for the Key Management Infrastructure (KMI) Management Client (MGC) Node
Yes/No/NA	w. Operational Security Doctrine for KG-250X – High Assurance Internet Protocol Encryptor (HAIPE)
Yes/No/NA	x. Process Security Doctrine for the Registration of KMI Operating Accounts and KMI Users

Yes/No/NA	y. Type 1 Certificate Policy (CP)
Yes/No/NA	z. MGC Operations and Maintenance Manual for the KMI Client Node

Commanding Officer: _____Manager:_____

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

TAB A SECTION 8 - REPORT RETENTION/DISPOSITION

Answer	Area/Item Reviewed
Yes / No	01. Are inactive records awaiting expiration of the required retention period clearly labeled with the classification, downgrading instructions and the authorized destruction date? [EKMS-1(Series), Article 715.c]
	02. Have the following been retained for the **minimum** retention period of **one (1) year**: [[EKMS-1 (Series) Annex M]
Yes / No	a. Receipts for official messenger mail, DCS courier mail and registered mail
Yes / No	b. Terminated Letters of Agreement
Yes / No	c. Closed out Visitor's Register
	Have the following been retained for the **minimum** retention period of **two (2) years**: [EKMS-1 (Series) Annex M]
Yes / No	b. General correspondence and messages pertaining to COMSEC matters or holdings?
Yes/No/NA	c. LMD/KP PIN/CIK log
Yes / No	d. Spot Checks(or log)/Self-Assessments
Yes / No	e. Messages, letters or memorandums used to document or report COMSEC Incidents or PDSs **Note:** If an incident or PDS is self-discovered but no documentation exists to indicate it was reported to the unit CO or externally, as applicable, it must be documented and reported.
Yes / No	03. Have the following been retained for the **minimum** retention period of **two (2) years** (current year plus previous 2 full years):
	a. Inventory Reports (SAIRS, CCIRSs, Combined) for all material **Note:** working copies can be purged upon receipt of a RCC.
Yes / No	b. Other accounting reports [Conversion, Generation, Possession, Relief from Accountability, Transfer and Destruction Reports (to include; Reportable Destruction Reports for ALC-1, 2, and 6 material Destruction Reports for ALC-4/7 material, and working copies of SF-153s generated for account/LE destruction)? **Note:** For material reflected in Tier 1 as "In Stock" the account must have the material or Destruction, ROA or Transfer Report.

Commanding Officer: _____Manager:_____

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

TAB A SECTION 9 - RESEALING/STATUS MARKINGS/PAGE CHECKS/CORRECTIONS AND AMENDMENTS

Answer	Area/Item Reviewed
Yes/No/NA	01. Has unsealed COMSEC material been sealed or resealed in accordance with EKMS-1 (Series) and local command instruction(s)? [EKMS-1 (Series), Articles 769.g, 772.a & .b, 945.d, 1005.a]
Yes/No/NA	02. For accounts with less than 500 line items, are effective and supersession dates annotated on all physical COMSEC keying material, COMSEC accountable manuals and publications, as applicable? [EKMS-1 (Series), Article 760.a]
Yes/No/NA	03. Are keytape canisters free of locally applied labels which may conceal attempted penetration or prevent COR Audit of protective packaging, as applicable? [EKMS-1 (Series), Article 760.e, 945.e]
Yes / No	04. Is effective and supersession information maintained within LCMS/MGC as applicable? [EKMS-1 (Series), Article 760.a; EKMS-1(SERIES) Supp-1, Article 709.c]
	05. Are required page/verification checks being accomplished by a manager and witness as follows: [EKMS-1 (Series), Articles 757.a, 775.e, and Annex P]
Yes/No/NA	a. Unsealed COMSEC keying material: upon initial receipt; during account inventories; during watch inventories; prior to transfer; and upon destruction?
Yes/No/NA	b. Unsealed maintenance and operating manuals: 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?
Yes/No/NA	c. Unsealed amendments: upon initial receipt; after entry of amendments which change pages (both person entering and person verifying entry); during inventories; during watch inventories; prior to transfer; and upon destruction?
Yes/No/NA	d. Maintenance and repair kits: upon initial receipt; upon installation of modification; during inventories; prior to transfer of the Q(repair kits); and upon destruction?
Yes/No/NA	e. Equipment: upon receipt (i.e., uncrating); during account and watch inventories; prior to transfer; and upon destruction?
Yes/No/NA	f. Resealed keying material: during account inventories; prior to transfer; and upon destruction?
Yes/No/NA	06. Are page checks of amendment residue recorded on the Record of Page checks (ROP) page? [EKMS-1 (Series), Article 757.d, 787.g]
Yes/No/NA	07. Are page check discrepancies being reported? [EKMS-1 (Series), Articles 757.h, 945.e, 1015; Annex O]
Yes/No/NA	08. Are corrections to a publication made with black or blue-black ink only? [EKMS-1 (Series), Article 787.g]

Yes/No/NA	09. 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]
Yes/No/NA	10. Has the person entering the amendment signed and dated the appropriate blanks on the publications Record of Amendments page [EKMS-1 (Series), Article 787.g]
Yes/No/NA	11. 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]
Yes/No/NA	12. Is classified & unclassified amendment residue destroyed within five days of amendment entry? [EKMS-1 (Series), Articles 540.g, 945.e]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 10 – SECURE TERMINAL EQUIPMENT (STE)/IRIDIUM/ OVER-THE-AIR-REKEY (OTAR)/OVER-THE-AIR TRANSFER (OTAT) & DATA TRANSFER DEVICE (DTD)/SIMPLE KEY LOADER (SKL)/TACTICAL KEY LOADER (TKL) & MODERN KEY

Answer	Area/Item Reviewed
Yes / No	01. Is access to Terminal Privilege Association (TPA) cards restricted to the Manager, Alternates or other properly designated personnel (LE Issuing) [EKMS-1 (Series), Annex T, paragraph 4]
Yes / No	02. Does the TPA or EKMS Manager, as applicable inspect STE Tamper Seals at a minimum of semi-annually in conjunction with inventories? [EKMS-1 (Series), Annex T paragraph 4.g]
Yes / No	03. Is keying material successfully filled in KSV-21 cards reflected on the account's reportable destruction report NLT 5th day of the month following the loading as "Filled in End Equipment" [EKMS-1 (Series), Article 1005.a; Annex T paragraph 17]
Yes / No	04. Are destruction reports submitted to the COR via the X.400 or PRSN as applicable; (1) Upon destruction of STE keying material when the KSV-21 card is filled/loaded from the MGC/AKP **or** (2) When an unused FD (filled by the CF) is loaded into a terminal for the express purpose of zeroizing it? [EKMS-1 (Series), Article 792; Annex T, paragraph 21]
Yes / No	05. Are in use STE/SCIP products rekeyed at a minimum of annually? [EKMS-1 (Series), Article 1005.a]
Yes/No/NA	06. Are KSV-21 cards issued to residential users filled with key which properly indicates the location as a **residence**? [EKMS-1 (Series), Annex T, paragraph 13.a]
Yes/No/NA	07. If the account generates, transmits, relays or receives electronic key, are local accounting records used and retained? [EKMS-1 (Series), Articles 1005.a, 1135; Annex M]
Yes/No/NA	08. Does the Manager conduct periodic reviews of OTAT/OTAR local accounting logs? [EKMS-1 (Series), Article 1105]
Yes / No	09. If T.S. key is stored in the device, is the device handled, stored and safeguarded under TPI? [CNSSI-3021, DOC 005-15]
Yes / No	10. Is unrestricted access to Supervisory CIKs or SSO passwords for the DTD/SKL/TKL or Talon Cards, limited to only those individuals who are authorized to perform all of the associated privileges? [CNSSI 3021, DOC 005-15]
Yes / No	11. Does the Manager or Supervisory User locally account for all CIKs by serial number or quantity, as applicable? [CNSSI 3021; DOC 005-15; DOC 024-12]

Yes / No	12. For non-watch station environments, are Supervisory and User CIKs inventoried whenever the account conducts Fixed-Cycle or Change of Manager inventories? [EKMS-1 (Series) Article 1005.a; CNSSI 3021; DOC 024-12; DOC 005-15]
Yes / No	13. Is audit trail data reviewed by a Supervisory User/SSO or Manager per the periodicity set forth in the respective Operational Security Doctrine (OSD) for the device and are audit trail reviews recorded in an Audit Review Log and retained for 2 years? [EKMS-1 (Series), Annex M; CNSSI 3021, DOC 024-12, DOC 005-15]
Yes / No	14. Are DTDs, SKLs or TKLs which are initialized or storing key reinitialized at a minimum of annually? [EKMS-1 Series), Article 945.c; CNSSI 3021, DOC 005-15, DOC 024-12]
Yes/No/NA	15. Are local accounting procedures in place to document HAIPE-TO-HAIPE Key Transfers (HtHKT), if performed? [EKMS-1 (Series), Article 1005.a; Annex U Para 8]
Yes / No	16. Has the Manager submitted the proper Central Facility (CF) forms to establish ordering privileges? i.e., CF Form 1205, CF Form 1206? [EKMS-1 (Series), Annex U, Para 3]
Yes / No	17. Has the KOAM, CPA or SA visually inspected INE holographic labels upon receipt or if discovered tampered? [EKMS-1 (series), EKMS-1(SERIES) Supp-1, Article 705.e]
Yes / No	18. Are FTRs registered as ALC-1, material type "Equipment"? [EKMS-5 (Series), Article 107]
Yes / No	19. Does the Manager ensure Modern Key filled in End Cryptographic Units (ECUs) is deleted from the DTD, SKL, or TKL by LE personnel following loading; recorded in LCMS as "Filled in End Equipment"; and reflected on the accounts end of month destruction report? [EKMS-1 (Series), Article 1005.a; Annex U, paragraph 8.c] **Note:** Late Destruction is only an incident if it involves physical or NATO material.
Yes / No	20. Does the Manager make use of the Modern Key Tracking Tool? Annex U, paragraph 8.d]
Yes / No	21. Does the Manager ensure unused Modern Key stored in a SKL or TKL is reported as destroyed by LE personnel when a device failure or database corruption occurs and is the keying material reflected on the end of the month destruction report? [EKMS-1 (Series), Article 1005.a; Annex U, paragraph 8.c]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 11 - EMERGENCY PROTECTION OF COMSEC MATERIAL

Answer	Area/Item Reviewed
Yes / No	01. Has the command prepared an Emergency Action Plan (EAP) for safeguarding COMSEC material in the event of an emergency? [EKMS-1, Annex H, paragraph 2]
Yes / No	02. Are all authorized personnel at the command/facility made aware of the existence of the EAP? [EKMS-1 (Series), Annex H, paragraph 6]
Yes / No	03. For commands, located within the U.S. and its territories, does the Emergency Action Plan (EAP) provide guidance detailing actions to be taken for natural disasters, civil/mob actions and terrorism? [EKMS-1 (Series), Annex H, paragraph 2]
Yes / No	04. Does the Manager maintain the COMSEC portion of the command EAP? [EKMS-1 (Series), Annex H, paragraph 1]
Yes/No/NA	05. For commands located outside U.S. and its territories, does the EAP provide detailed guidance for both natural disasters and hostile actions? [EKMS-1 (Series), Annex H, paragraph 2]
Yes / No	06. When planning for natural disaster, does the EAP provide for: [EKMS-1 (Series), Annex H, paragraph 4]
	a. Fire reporting and initial firefighting 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 exposures to appropriate authorities?
Yes / No	07. Are EAP training exercises conducted yearly to ensure that everyone is familiar with their assigned duties? [EKMS-1 (Series), Annex H, paragraph 6.d]
Yes / No	08. Is the CMWS/DMD PS addressed in the Emergency Action and/or Emergency Destruction Plan (EAP/ EDP), as applicable? [EKMS-1 (Series), Annex H; Annex W, paragraph 10]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 12 - EMERGENCY DESTRUCTION PLAN (EDP)

Note: Unless specified in Local, ISIC, or TYCOM directives, this section is only applicable to commands located outside the U.S. and its territories and deployable commands.

Answer	Area/Item Reviewed
Yes/No/NA	01. Does the COMSEC account have an EDP incorporated into their EAP? [EKMS-1 (Series), Annex H, paragraph 2.c]
Yes/No/NA	02. Does the EDP identify personnel assignments and the chain of authority that is authorized to make the determination that emergency destruction is to begin? [EKMS-1 (Series), Annex M, paragraph 5.d; SECNAV-M 5510.36, exhibit 2B]
Yes / No	03. Are devices and facilities for the emergency destruction of COMSEC material readily available and in good working order? [EKMS-1 (Series), Annex M, paragraphs 5.d, 6.c]
Yes/No/NA	04. 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]
Yes / No	05. Are the priorities of destruction indicated in the plan? [EKMS-1 (Series), Annex M, paragraph 8]
Yes / No	06. Are EAP/EDP training exercises conducted on an annual basis to ensure that everyone is familiar with their duties? [EKMS-1 (Series), Annex H, paragraph 6]
Yes / No	07. Is the EDP divided into two parts: one for precautionary and one for complete destruction? [EKMS-1 (Series), Annex H, paragraph 7]
Yes / No	08. Does the EDP provide for adequate identification and rapid reporting of the material destroyed, to include the method and extent of destruction and any classified COMSEC material items presumed compromised? [EKMS-1 (Series), Annex H, paragraph 10]
Yes / No	09. Does the EDP stress that accurate reporting of information concerning the extent of the emergency destruction is second in importance only to the destruction of the material itself? [EKMS-1 (Series), Annex H, paragraph 10]
Yes/No/NA	10. Are document sinking bags available in sufficient quantity and in good condition to permit jettison of COMSEC material? (**Note:** Surface units only) [EKMS-1 (Series), Annex H, paragraph 9.d]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 13 - COMMANDING OFFICER (CO, OIC, (SCMSRO) RESPONSIBILITIES

Answer	Area/Item Reviewed
Yes / No	01. Has the Commanding Officer:
	a. appointed, in writing, qualified and responsible individuals as EKMS/KOA Manager and Alternate Manager(s), Local Elements (Issuing), and, if desired a Clerk. [EKMS-1 (Series) Article 450.b; EKMS-1(SERIES) Supp-1, Article 405.d]
Yes / No	b. established, in writing, a list of personnel authorized access to keying material. [EKMS-1 (Series), Article 450.c]
Yes / No	c. ensured that training procedures are adequate to meet operational requirements. [EKMS 1 (Series), Article 450.d; EKMS-1(SERIES) Supp-1 Article 603.a]
Yes / No	d. ensured that COMSEC incident reports are promptly submitted and action taken as required. [EKMS-1 (Series), Articles 450.e, 960]
Yes/No/NA	e. Only extended crypto periods as authorized, up to two hours. [EKMS-1 (Series), Article 450.f]
Yes / No	f. ensured that local procedures were established for identification and reporting of any potentially significant changes in life-style, financial status, or disciplinary problems involving personnel authorized access to COMSEC material. [EKMS-1 (Series), Article 450.h; SECNAV M5510.30 Articles 7-2.C, 10-1.2; Exhibit 10A]
Yes / No	g. ensured that quarterly spot checks are conducted where COMSEC material is used and stored. [EKMS-1 (Series), Articles 1005.a, 450.i]
Yes / No	h. received debriefings from CMS COR Audit Teams and CMS Auditors. [EKMS-1 (Series), Article 450.j]
Yes / No	i. ensured that the Emergency Action Plan (EAP)/ Emergency Destruction Procedures (EDP) were established and tested. [EKMS-1(Series,) Article 450.m]
Yes / No	j. ensured any collateral duties assigned to Manager did not interfere with COMSEC responsibilities. [EKMS-1 (Series), Article 450.o]
Yes / No	k. Has the CO, SCMSRO or OIC, as applicable received the EKMS for CO's training facilitated by their local CMS COR Audit Team? [EKMS-1 (Series), Article 325.c]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 14 - CLIENT PLATFORM ADMINISTRATOR (CPA), CLIENT PLATFORM SECURITY OFFICER (CPSO), TOKEN SECURITY OFFICER (TSO) RESPONSIBILITIES – (THIS SECTION IS ONLY APPLICABLE TO KOAs)

Answer	Area/Item Reviewed
Yes/No/NA	01. Is the MGC compliant with mandatory software upgrades or IAVA patches? [EKMS-1(SERIES) Supp-1, Article 219.b]
Yes/No/NA	02. Has the CPA established and maintains unique Microsoft Windows user-accounts and permissions on the Client Host?
Yes/No/NA	03. If a system recovery is performed, are database backups and AKPREINIT drives used less than 7 calendar days old [EKMS 1B Supp-1, Articles 501.e, 903.b]
Yes/No/NA	04. Has the CPSO sent an exact copy of archived audit data to the Central Services Node (CSN) within 30 days of the archive? [EKMS 1B Supp-1, Articles 501.f, 903.a]
Yes/No/NA	05. Has the CPSO; exported the AKP Diagnostic History Log (DHL) to the MGC every 6 months or more frequently; reviewed the DHL for anomalies and documented the review? [EKMS-1(SERIES) Supp-1, Articles 501.f, 903.a]
Yes/No/NA	06. Does the CPSO verify the BIOS password in conjunction with each archive of audit data? [EKMS-1(SERIES) Supp-1, Articles 501.f, 903.a]
Yes/No/NA	07. Does the TSO conduct and document audit trail reviews at a minimum of every 90 days on active KOV-29s? [EKMS-1(SERIES) Supp-1, Articles 411.c, 805.c]
Yes/No/NA	08. Has the TSO created and issued a new password when a new Token SO is appointed? [EKMS-1(SERIES) Supp-1, Articles 215.a, 805.c]
Yes/No/NA	09. Does the TSO have a Compromise Recovery Plan (CRP) for KOV-29s associated with the Token SO password on file? [EKMS-1(SERIES) Supp-1, Article 215.a]
Yes/No/NA	10. Does the CRP discuss lost token to include revocation procedures? [EKMS-1(SERIES) Supp-1, Article 215.a]
Yes/No/NA	11. Is the TSO the TSO for their own token? [EKMS-1(SERIES) Supp-1 Articles 103.s, 305.n, 411.c, 805.b]

Commanding Officer: _____Manager:_____

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

TAB A SECTION 15 – COMSEC MANAGEMENT WORKSTATION DATA MANAGEMENT DEVICE POWER STATION (CMWS/DMD PS)

Answer	Area/Item Reviewed
Yes/No/NA	01. Do personnel with access to the CMWS/DMD PS possess a minimum SECRET security clearance (current within 10 years)? [EKMS-1 (Series), Annex W paragraphs 4, 5, and 11]
Yes/No/NA	02. Is the CMWS/DMD PS compliant with SSC-LANT issued Information Security Vulnerability Assessment (IAVA) patches? [EKMS-1 (Series), Annex W paragraph 11]
Yes/No/NA	03. Is use of the CMWS/DMD PS restricted to "Black Key" only? [EKMS-1 (Series), Annex W, paragraph 3.b]
Yes/No/NA	04. Is there evidence of unauthorized access or connections to the CMWS/DMD PS? [EKMS-1 (Series) Annex W paragraphs 3.c, 3.d, 5.h, 11]
Yes/No/NA	05. Does each CMWS/DMD PS user have a unique user ID/password and are passwords changed at a minimum of every 90 days? [EKMS-1 (Series), Annex W paragraphs 5.d, 11] **Note:** Shared accounts and/or passwords must be assessed as a COMSEC incident; failure to change passwords every 90 days or more frequently should be addressed as a PDS.

Commanding Officer: _____Manager:_____

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

TAB B SECTION 1 - SECURITY

Answer	Area/Item Reviewed
Yes / No	01. Are adequate visitor controls enforced to ensure that access to classified information is given only to visitors who possess the proper identification, proper security clearance, and NEED TO KNOW? [SECNAV-M 5510.30 (Series), Article 11-1 paragraph 2, 3; SECNAV-M 5510.36, Article 7-12; EKMS-1 (Series), Article 550.e]
Yes / No	02. Is a visitor's register properly maintained (all fields completed) and retained for one year from the last date recorded? () [EKMS-1 (Series), Article 550.e, Annex M]
Yes/No/NA	**a. For USMC units only.** Does the "Restricted Area" sign meet the criteria set forth in MCO 5530.14? [MCO 5530.14 (Series), Article 3004]
Yes / No	03. Is unescorted access limited to individuals whose duties require access and who meet access requirements? [EKMS-1 (Series), Article 505]
Yes / No	04. Are the names of individuals with regular duty assignments in the COMSEC facility on a formal access list? [EKMS-1 (Series), Article 550.e]
Yes / No	a. Are personnel whose duties require access to COMSEC material formally authorized in writing by the CO/OIC/SCMSRO? [EKMS-1 (Series), Article 505.d, 550.e]
Yes / No	b. If personnel are authorized access to COMSEC material on an access list, has the list been updated annually or whenever the status of an individual changed? [EKMS-1 (Series), Article 505.d]
Yes / No	05. Are security clearances for personnel who require access to classified COMSEC material equal to or higher than the material the member has access to and within scope? [EKMS-1 (Series) Articles 505, 945.e]
Yes / No	06. If keying material is held/used to protect SCI/SI information, are LE personnel with access to the keying material or devices storing the keying material SCI eligible and indoctrinated? [EKMS-1 (Series), Articles 414.d, 945.e]
Yes / No	07. Is the exterior of each COMSEC security container free of markings which reveal the classification or description of the material stored in the container? [SECNAV-M 5510.36, Article 10-1, paragraph 3]
Yes / No	08. Are applicable security controls (e.g., guards and alarms) in place? [SECNAV-M 5510.36, Chapter 10; EKMS-1 (Series), Article 520.a; MCO 5530.14 (Series), 3003]
Yes / No	09. Do storage containers meet the minimum security requirements for the highest classification of keying material stored therein? [EKMS-1 (Series), Article 520.d; SECNAV-M 5510.36, Chapter 10]

Yes / No	10. Is a Maintenance Record for Security Containers and Vault Doors (Optional Form 89) maintained for each security container, used to record damages, repairs or alternations and retained within the container? EKMS-1 (Series) Article 520.b; SECNAV-M5510.36 Article 10-15]
Yes / No	11. If TOP SECRET material is held by the LE, do storage containers conform to two person integrity (TPI) requirements? [EKMS-1 (Series), Article 520.e]
Yes / No	12. Is a Security Container Information Form (SF 700) maintained for each lock combination and placed in each COMSEC security container? [SECNAV-M 5510.36, Article 10-12, paragraph 3; EKMS-1 (Series), Article 520.b]
Yes / No	13. Is a Security Container Check Sheet (SF-702) maintained for each lock combination of a COMSEC storage container? [SECNAV-M 5510.36, Article 7-10; EKMS-1 (Series), Article 520.b]
Yes / No	14. Are completed SF-702s retained for 30 days beyond the last date recorded? [EKMS-1 (Series] Article 520.b, Annex T paragraph 2.a; SECNAV-M5510.36 Article 7.11]
Yes / No	15. Except in an emergency, are combinations to security containers used by the LE restricted to properly cleared and authorized LE personnel only? [EKMS-1 (Series), Article 515.c]
Yes/No/NA	16. If the COMSEC facility is **continuously** manned, are security checks conducted at least once every 24 hours and documented on a SF-701? [EKMS-1 (Series), Article 550.d]
Yes/No/NA	17. In a **non-continuously** manned COMSEC facility, are security checks conducted prior to departure of the last person and documented on an Activity Security Checklist (SF-701)? [EKMS-1 (Series), Article 550.d; SECNAV-M 5510.36, Article 7.11]
Yes / No	18. Are completed SF-701s retained for 30 days beyond the last date recorded [EKMS-1 (Series] Article 550.d, Annex T paragraph 2; SECNAV-M5510.36 Article 7.11]
Yes / No	19. 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 and documented on a SF-701 to ensure that all doors are locked and that there have been no attempts at forceful entry. [EKMS-1 (Series), Article 550.d]
Yes / No	20. Are combinations & associated SF-700s for TPI containers completed, stored, and safeguarded to prevent a single person from having access to both combinations? [EKMS-1 (Series), Article 510.c]
Yes / No	21. Are sealed records of combinations to COMSEC containers maintained in an approved security container (other than the container where the COMSEC material is stored), and available to duty personnel for emergency use? [EKMS-1 (Series), Article 515.e; 945.e]
	22. Are SF-700s protected as follows: [EKMS-1 (Series), Article 515.f]

Yes / No	a. Individually wrapped in aluminum foil and protectively packaged in an SF-700 envelope?
Yes / No	b. Are SF-700s sealed using transparent lamination or plastic tape?
Yes / No	c. Names of individuals authorized access to the combinations recorded on the front of the envelope?
Yes / No	d. Proper classification and downgrading instructions on envelope?
Yes / No	e. Are the envelopes inspected monthly to ensure they have not been tampered with and the COR Audit findings documented on a locally generated log?
Yes / No	f. Are combinations to COMSEC containers changed when initially placed in use, taken out of service, at least biennially, upon transfer/reassignment of personnel who have access, or when compromised? EKMS-1 (Series), Article 515.b]
Yes / No	23. 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; Annex H, paragraph 3]
Yes / No	24. Is COMSEC material properly stored when not in use or under the direct control of authorized personnel? [EKMS-1 (Series), Article 520.a]
Yes / No	25. Are COMSEC files, records and logs handled and stored in accordance with their overall classification? [EKMS-1 (Series), Article 715.a; SECNAV-M 5510.36, Article 6-3, 6-26]
Yes / No	26. Do classified COMSEC files, records and logs reflect proper classification markings, the derivative source for the classification and declass/downgrading instructions? [EKMS-1 (Series), Article 715.d]
Yes/No/NA	27. If contractor personnel are assigned to and have access to COMSEC material, does the command have a valid (not-expired) DD-254 and does Block 10 indicate the access is required? [EKMS-1 (Series) Article 505.g]
Yes / No	28. Are in-use In-Line Network Encryptors (INEs) such as KG-175s, KG-250s, or KIV-7Ms compliant with **NSA directed mandatory software upgrades** and if not, has DIRNSA or NCF issued an official waiver, in writing? [EKMS-1 (Series) Article 945.c] ***Randomly select 3 devices issued to LEs and verify it is compliant with the latest version authorized and directed by NCMS via ALCOM message. Record the Short Title, Serial Number, and LE where the device is installed***

Commanding Officer: _____Manager:_____

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

TAB B SECTION 2 - LOCAL ELEMENT RESPONSIBILITIES

Answer	Area/Item Reviewed
Yes/No/NA	01. **LE Issuing only:** Are Alternate LE issuing personnel actively involved in the performance of LE issuing duties and ready at all times to manage the LE's COMSEC requirements in the absence of the LE Issuing? [EKMS-1 (Series), Article 414]
Yes/No/NA	02. **LE Issuing only:** Does the Primary (Issuing) LE provide the CO/OIC, SCMSRO and other interested personnel with general information about new or revised EKMS policies or procedures? [EKMS-1 (Series), Article 465.a]
Yes/No/NA	03. **LE Issuing only:** Does the (Issuing) LE maintain written instructions issued by the supporting COMSEC account governing the handling, accountability, and disposition of COMSEC material? [EKMS-1 (Series), Article 465.b]
Yes/No/NA	04. **LE Issuing only:** Does the LE provide written guidance concerning accountability, handling, and disposition of COMSEC material to all LE (Using) personnel [EKMS-1 (Series), Article 465.c]
Yes/No/NA	05. Have all USN (military) LE personnel completed the applicable qualification level of the (NAVEDTRA 43462 series) Personnel Qualification Standards (PQS)? [EKMS-1 (Series), Articles 312, 410]
Yes / No	06. **LE Issuing only:** Does the LE issuing conduct monthly training with all personnel handling COMSEC material to ensure they are adhering to proper EKMS procedures and document training in accordance with command directives? (EKMS-1 (Series), Article 465.c; Annex M paragraph 2]
	07. Are or have;
Yes / No	a. LE personnel authorized access to keying material in writing
Yes / No	b. Completed a SD Form 572 and is such retained for 90 days from the date the individual no longer requires access to COMSEC material (is reassigned, transfers, etc…)?
Yes/No/NA	c. If the (Issuing) LE has LEs which are responsible to a CO other than the Primary (Issuing) LE's CO, has the Primary (Issuing) LE ensured that Letters of Agreement were exchanged? [EKMS-1 (Series), Article 445, Annex G]
	08. Does the Letter of Agreement address the minimum issues: [EKMS-1 (Series), Annex G]
Yes / No	a. Compliance with locally prepared COMSEC instructions?
Yes / No	b. COMSEC Incident and PDS documentation and reporting procedures?

Yes / No	c. Responsibility for certifying clearance/ access?
Yes / No	d. The issuance of COMSEC material in electronic form?
Yes / No	e. Notification of Local Element Appointments?
Yes / No	f. Storage/Facility Clearance?
Yes / No	09. Is a copy of the signed, Letter of Agreement held by the LE and retained as required? [EKMS-1 (Series), Article 709.c, Annex M]
Yes/No/NA	10. **LE Issuing only.** Does the Primary (Issuing) LE ensure that all cryptographic maintenance personnel that perform maintenance within his/her account, have DD 1435(s) documented and on file and are designated in writing by the Commanding Officer? [EKMS 5 (Series), Article 111]
Yes/No/NA	11. **LE Issuing only.** Has a formal Letter/Memorandum of Appointment (LOA/MOA) been completed and signed by the CO for the Primary (Issuing) LE and Alternate(s)? [EKMS-1 (Series), Article 418; Annex F] **Note:** (1) The absence of an appointment letter when the person has the combinations at the LE Issuing level would constitute "unauthorized access" for a LE Issuing or Alternate. (2) If the LE Issuing/Alternate is appointed in writing but the letter was signed by a previous CO and the command had a change of command within 60 days and updated letters are pending signature, assess as an Administrative discrepancy.
Yes/No/NA	12. **LE Issuing only.** Does the Primary (Issuing) LE and Alternates meet the minimum designation requirements specified in EKMS-1 (Series)? [EKMS-1 (Series), Article 414]
Yes/No/NA	13. **LE Issuing only.** Has the LOA/MOA been forwarded to the parent account EKMS Manager and a copy retained on file for a minimum of 2 years following the relief of the Primary (Issuing) LE and/or Alternates? [EKMS-1 (Series), Art. 418, Annexes F and M]
Yes/No/NA	14. **LE Issuing only.** Does the (Issuing) LE maintain required files as directed by the parent account EKMS Manager? [EKMS-1 (Series), Article 703]
Yes/No/NA	15. **For external LEs supported through a LOA only.** Are inventories completed for Change of Command, (OIC) or LE Issuing (as applicable?) [EKMS-1 (Series) Articles 450, 465, 766.a, 1005.a]
Yes / No	16. Do LE personnel have access to written guidance (provided by the account Manager) concerning the proper handling, accountability, and disposition of COMSEC material? [EKMS-1 (series), Article 455.e]

Yes / No	17. **For external LEs supported through a LOA only.** Does the Commanding Officer or OIC, as applicable conduct a minimum of (1) spot check per quarter within their organization? [EKMS-1(Series) Articles 450.i, 465] **Note:** External LEs refers to those assigned to a Detachment of the parent account command with an OIC or a different unit (CO other than the one responsible for the account) supported through a LOA/MOU

Commanding Officer: _____Manager:_____

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

TAB B SECTION 3 – ACCOUNTABLE ITEM SUMMARY & LOCAL CUSTODY FILE, INVENTORIES, PAGECHECKS & AMENDMENTS

Answer	Area/Item Reviewed
Yes/No/NA	01. **For LE Issuing only.** Does the LE Issuing maintain an up to date Accountable Item (A/I) Summary provided by the parent account COMSEC Manager? [EKMS-1 (Series), Article 763.c]
Yes / No	02. Does the LE maintain a local custody file which contains signed, effective local custody documents for each item of COMSEC material issued from the supporting account? [EKMS-1 (Series), Article 712, 945.e]
Yes/No/NA	03. **For LE Issuing only.** Do local custody documents (i.e., SF 153, or locally prepared equivalent), contain the minimum required information? [EKMS-1 (Series), Article 769.c]
Yes / No	04. Are inactive files/records labeled to reflect the authorized date of destruction? [EKMS-1 (Series), Article 715.c]
Yes/No/NA	05. **Are inventories for non-watch station and watch station environments** conducted and recorded on the local custody issue document(non-watch stations only) or a watch-to-watch inventory maintained and lists all COMSEC material held (including accountability for resealed segments and CIKS for DTDs, SKLs or TKLs issued)? [EKMS-1(Series), Article 775.d, 778.c, Annex T]
Yes/No/NA	06. Is material reflected on the watch-to-watch inventory listed by short title, edition, accounting number (if applicable) and quantity? [EKMS-1 (Series), Article 775.d, 1005.a]
Yes/No/NA	07. Has the inventory been properly signed and dated for each change of watch? [EKMS-1 (Series), Article 775.d, 1005.a]
Yes/No/NA	08. Are watch-to-watch inventories being retained for 30 days beyond the last recorded date on the inventory? [EKMS-1 (Series), Annex M, paragraph j]
	09. Are required page checks being accomplished as follows: [EKMS-1 (Series), Article 775.e, 778.d; Annex P]
Yes/No/NA	a. Unsealed COMSEC keying material. Upon initial receipt; during account and watch inventories; and prior to destruction?
Yes/No/NA	b. Resealed keying material. During Fixed-Cycle and Change of EKMS/KOA Manager inventories; and upon destruction?
Yes/No/NA	c. Unsealed maintenance and operating manuals. Upon initial receipt; after entry of an amendment which changes pages; during Fixed-Cycle and Change of EKMS/KOA Manager inventories; and upon destruction?

Yes/No/NA	d. Equipment. Upon initial receipt (uncrating); during Fixed-Cycle and Change of EKMS/KOA Manager inventories; during watch inventories; and upon destruction?
Yes/No/NA	10. Are page check discrepancies being reported? [EKMS-1, Articles 757.h, 945.e, 1015; Annex O]

Commanding Officer: _____Manager:_____

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

TAB B SECTION 4 - RESEALING/STATUS INFORMATION/CORRECTIONS & AMENDMENTS

Answer	Area/Item Reviewed
Yes/No/NA	01. If keying material was unintentionally removed from its protective canister, is the following recorded on the CMS-25: [EKMS-1(Series), Articles 772.d, 945.e, 1005.a]
Yes/No/NA	a. A statement the keytape segment(s) were unintentionally removed?
Yes/No/NA	b. The date of the removal?
Yes/No/NA	c. Identity of the keytape segment(s) actually removed?
Yes/No/NA	d. Signatures of the individuals who removed the key?
Yes/No/NA	02. Are users provided and maintain up-to-date status information to ensure usage and destruction occurs when required by the Controlling Authority or Command Authority, as applicable? [EKMS-1 (Series) Articles 465, 540, 790, 945]
Yes/No/NA	03. Are the effective and supersession dates annotated on all COMSEC; keying material, accountable manuals and publications in accordance with EKMS-1? [EKMS-1 (Series), Articles 760.a, 775.g]
Yes/No/NA	04. Are key tape canisters free of locally applied labels and stickers which may conceal attempted penetration or prevent COR Audit of protective packaging? [EKMS-1 (Series), Articles 760.e, 760.f, 945.e] **Note**: If discovered, remove label, inspect the canister and train the user. If the canister is damaged, report as a Physical Incident.
Yes/No/NA	05. Are corrections to publications made with black or blue-black ink only? [EKMS-1 (Series), Article 787.g]
Yes/No/NA	06. Is each pen and ink correction identified by writing the correction number in the margin opposite the correction? [EKMS-1 (Series), Article 787.g]
Yes/No/NA	07. 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]
Yes/No/NA	08. 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]
Yes/No/NA	09. 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), Article 787.g]

Commanding Officer: _____Manager:_____

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

TAB B SECTION 5 – ROUTINE DESTRUCTION

Answer	Area/Item Reviewed
Yes / No	01. Are local destruction records being completed to document destruction of all Top Secret and Secret COMSEC material and all AL1 and AL2 material regardless of its classification? [EKMS-1 (Series), Article 736.b, Article 945.e]
Yes / No	02. Do local destruction records for segmented COMSEC material contain the following: [EKMS-1 (Series), Chapter 7, Article 715.d, fig 7-1, 7-2, 7-3]
Yes / No	a. Short title and complete accounting data?
Yes / No	b. Date of destruction?
Yes / No	c. Signatures of the two individuals conducting destruction?
Yes / No	d. Marked "CONFIDENTIAL (When filled in)"?
Yes / No	e. Classification and Declassification markings? Derived from: NSTISSI 4002 Declassify on: DD Month YYYY
Yes / No	03. Is 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 and Article 1005.a]
Yes / No	04. Are local destruction records [SF-153s] for COMSEC material maintained by the local element for 2 years past the destruction of the material? [EKMS-1 Series), Figure 7-1-3, Articles 712.a, 945.e, Annex M, paragraph 2.a]
Yes / No	05. Is destruction of key issued either physically or in electronic form (DTD, SKL, TKL) completed within the prescribed timeframes (EKMS-1 (Series), Articles 540, 778.c, 1005.a]
Yes / No	06. Can LE personnel demonstrate the proper procedures for conducting routine destruction of COMSEC material? [EKMS-1 (Series), Articles 540, 790; CNSSI 3021; DOC 024-12; DOC 005-15]
Yes/No/NA	07. If the LE has experienced a corrupted/failed DTD, SKL, or TKL storing modern key, did the LE submit a manual SF-153 destruction report to the LE Issuing/supporting COMSEC Account Manager, as applicable? [EKMS-1 (Series), Annex U paragraph 8.c; Article 1005.a]

Commanding Officer: _____Manager:_____

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

TAB B SECTION 6 - OVER-THE-AIR-REKEY/OVER-THE-AIR TRANSFER & DATA TRANSFER DEVICE (DTD)/SIMPLE KEY LOADER(SKL)/TACTICAL KEY LOADER (TKL), MANAGEMENT OF MODERN KEY AND THE COMSEC MANAGEMENT WORKSTATION DATA MANAGEMENT DEVICE POWER STATION (CMWS/DMD PS)

Answer	Area/Item Reviewed
Yes/No/NA	01. If the LE has a KOK-23, are PINS changed every 90 days or more frequently, when required? [DOC 027-09 paragraph 9; EKMS-1 (Series) Article 1005.a]
Yes/No/NA	02. If the LE generates, receives, relays, or transmits electronic key for OTAD, OTAR or OTAT, are accounting records used and maintained for a minimum of 60 days following the date of the last entry? [EKMS-1 (Series), Articles 1005.a, Annex M]
Yes/No/NA	03. If Top Secret key is stored in a DTD, SKL, etc… is the device, handled, stored and safeguarded under TPI? [EKMS-1 (Series) Article 510; CNSSI-3021; DOC 005-15]
Yes/No/NA	04. Is unrestricted access to Supervisory CIKs or the SSO password for the DTD/SKL/TKL, as applicable, limited to only those individuals who are authorized to perform all of the associated privileges? [CNSSI 3021; DOC 024-12; DOC 005-15]
Yes/No/NA	05. Have recipients of electronic key issued to either a DTD/SKL/TKL signed a local custody document acknowledging receipt of the key? [EKMS-1 (Series), Articles 769.h, 945.e]
Yes/No/NA	06. Does the Manager or Supervisory User locally account for CIKs by serial number or quantity, as applicable? [CNSSI 3021; DOC 005-15; DOC 024-12]
Yes/No/NA	07. **For non-watch station environments**, are Supervisory and User CIKs inventoried whenever the account conducts Fixed-Cycle or Change of Manager inventories? [EKMS-1 (Series) Article 1005.a;CNSSI 3021;DOC 024-12;DOC 005-15]
Yes/No/NA	08. Is audit trail data reviewed by a Supervisory User/SSO or Manager per the periodicity set forth in the respective Operational Security Doctrine (OSD) for the device and are audit trail reviews recorded in an Audit Review Log and the log on file for 2 years? [EKMS-1 (Series) Article 465, Annex M; CNSSI 3021, DOC 024-12, DOC 005-15]
Yes/No/NA	09. Are DTDs, SKLs or TKLs which are initialized or storing key reinitialized at a minimum of annually? [EKMS-1 Series), Article 945.c; CNSSI 3021, DOC 005-15, DOC 024-12]
Yes/No/NA	10. Are HAIPE or SCIP devices rekeyed at a minimum of annually? [EKMS-1 (series) Article 1005.a; Annex T, paragraph 5.h]

Yes/No/NA	11. For **non-watch station environments:** Are DTD/SKL or TKL CIKS, as applicable inventoried on days when the security container the devices are stored in is opened? [EKMS-1 (Series), Articles 778.c, 1005.a; CNSSI 3021, DOC 024-12, DOC 005-15]
Yes/No/NA	12. For **watch station** environments: Are CIKS for the DTD, SKL or TKL inventoried by serial number (DTD) or quantity/association (SKL/TKL) verified whenever watch personnel change? [EKMS-1 Series); Article 1005.a; CNSSI 3021, DOC 024-12, DOC 005-15]
Yes / No	13. Are DTDs, SKLs or TKLs free of any cracks or breaches in the housing? [EKMS-1 (Series) CNSSI 3021, DOC 024-12, DOC 005-15]
Yes / No	14. Do LE personnel ensure Modern Key filled in End Cryptographic Units (ECUs) is deleted from the DTD, SKL, or TKL following loading and reported to the COMSEC Account Manager as filled in end equipment? [EKMS-1 (Series), Article 1005.a; Annex U, paragraph 8.c]
Yes / No	15. Does the LE have a matrix or make use of the NCMS Modern Key Tracking tool to ensure INEs are not operating on expired key? [EKMS-1 (Series) Annex U, paragraph 8.b]
Yes / No	16. Do LE personnel submit a destruction report to the COMSEC Account Manager when a DTD, SKL or TKL failure occurs [EKMS-1 (Series), Article 1005.a; Annex U, paragraph 8.c]
Questions 17 are only applicable to LEs who have a CMWS/DMD PS	
Yes/No/NA	17. Do personnel with access to the CMWS/DMD PS possess a minimum SECRET security clearance (current within 10 years)? [EKMS-1 (Series), Annex W paragraphs 4, 5, and 11]
Yes/No/NA	18. Is the CMWS/DMD PS compliant with SSC-LANT issued Information Security Vulnerability Assessment (IAVA) patches? [EKMS-1 (Series), Annex W paragraph 11]
Yes/No/NA	19. Is use of the CMWS/DMD PS restricted to "Black Key" only? [EKMS-1 (Series), Annex W, paragraph 3.b]
Yes/No/NA	20. Is there evidence of unauthorized access or connections to the CMWS/DMD PS? [EKMS-1 (Series) Annex W paragraphs 3.c, 3.d, 5.h, 11]
Yes/No/NA	21. Does each CMWS/DMD PS user have a unique user ID/password and are passwords changed at a minimum of every 90 days? [EKMS-1 (Series), Annex W paragraphs 5.d, 11] **Note:** Shared accounts and/or passwords must be assessed as a COMSEC incident; failure to change passwords every 90 days should be addressed as a PDS.

Commanding Officer: _____Manager:_____

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

TAB B SECTION 7 - EMERGENCY ACTION/EMERGENCY DESTRUCTION PLAN (EAP/EDP)

Answer	Area/Item Reviewed
Yes / No	01. Do all COMSEC users have access to the COMSEC portion of the command's EAP? [EKMS-1 (Series), Article 455.o, Annex H, paragraphs 2, 6]
Yes / No	02. Are EAP training exercises conducted annually? [EKMS-1 (Series), Annex H, paragraph 6.d]
Yes / No	03. For OCONUS and deployable units, does the EAP provide detailed guidance for natural disasters and hostile actions and include Emergency Destruction Procedures (EDP)? [EKMS-1 (Series), Annex H, paragraph 2.c]
Yes / No	04. Is the CMWS/DMD PS addressed in the Emergency Action and/or Emergency Destruction Plan (EAP/EDP), as applicable? [EKMS-1 (Series), Annex H; Annex W, paragraph 10]
Yes / No	05. When planning for natural disasters, does the EAP provide for: [EKMS-1(Series), Annex H, paragraph 4]
Yes / No	a. Fire reporting and initial firefighting by assigned personnel?
Yes / No	b. Assignment of on-the-scene responsibility for protecting COMSEC material held?
Yes / No	c. Protecting material when admitting outside fire fighters into the secure area(s)?
Yes / No	d. Securing or removing classified COMSEC material and evacuating the area(s)?
Yes / No	e. Assessing and reporting probable exposure of classified COMSEC material to unauthorized persons during the emergency?
Yes / No	f. Completing a post-emergency inventory of COMSEC material and reporting any losses or unauthorized exposures to appropriate authorities?
Yes / No	06. Does the LE have an Emergency Destruction Plan (EDP) incorporated into its EAP? [EKMS-1 (Series), Annex H, paragraph 2.c]
Unless specified in Local, ISIC, or TYCOM directives, questions 07 - 15 are only applicable to commands located outside the U.S. and its territories and deployable commands.	
Yes / No	07. Does the EDP identify personnel assignments and the chain of authority authorized to make the determination that emergency destruction is to begin? [EKMS-1 (Series), Annex H, paragraph 5.d]
Yes / No	08. Are devices and facilities for the emergency destruction of COMSEC material readily available and in good working order? [EKMS-1 (Series), Annex H, paragraph 5.d and 6.c]

Yes/No/NA	09. 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 H, paragraph 5.e]
Yes / No	10. Are the priorities of destruction indicated in the plan? [EKMS-1 (Series), Annex H, paragraph 8]
Yes / No	11. Is the EDP divided into two parts: one for precautionary and one for complete destruction? [EKMS-1 (Series), Annex H, paragraph 7]
Yes / No	12. Does the EDP provide for the adequate identification and rapid reporting of the material destroyed, to include the method and extent of destruction? [EKMS-1 (Series), Annex H, paragraph 10]
Yes / No	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 H, paragraph 10.a]
Yes/No/NA	14. **Surface units only:** Are document sinking bags available in sufficient quantity and in good condition to permit jettison of COMSEC material? [EKMS-1 (Series), Annex H, paragraph 9.d]
Yes/No/NA	15. If the user deploys in aircraft, does the plan cover specific actions to be followed in aircraft? [EKMS-1 (Series), Annex H, paragraph 9.c]

Commanding Officer: _____Manager:_____

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